VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

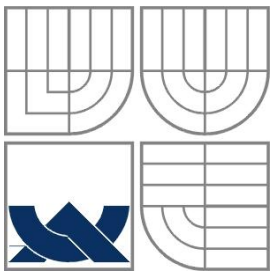
FORENZNÁ ANALÝZA V OPERAČNÝCH SYSTÉMOCH LINUX

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

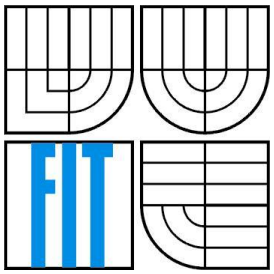
AUTOR PRÁCE
AUTHOR

MARTIN BENEŠ

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

FORENZNÍ ANALÝZA V OPERAČNÍCH SYSTÉMECH LINUX

FORENSIC ANALYSIS IN LINUX OS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
MARTIN BENEŠ

VEDOUCÍ PRÁCE
SUPERVISOR
ING. PAVEL OČENÁŠEK, PH.D.

BRNO 2012

Abstrakt

Práce se zabývá rozborem možností forenzní analýzy při vyšetřování na operačních systémech Linux. Použitím distribuce BackTrack a obsažených nástrojů je provedeno forenzní vyšetřování na testovací instalaci operačního systému Xubuntu. Práce je rozdělena do kapitol, kde postupně popisuje základy operačního systému Linux, přes požadavky kladené na vyšetřovatele a jeho vybavení až k seznámení s nástroji používanými na analýzu. Všechny porovnávané nástroje jsou volně dostupné a svou velikostí sahají od jednoduchých nástrojů až po komplexní prostředí. Teoretické poznatky jsou aplikovány na reálný systém, kde je ukázáno použití analyzovaných nástrojů. Práce je zakončena shrnutím nálezů vyšetřování do forenzního posudku.

Abstract

This thesis deals with possibilities of forensic analysis on Linux operating system investigation. Forensic investigation is performed on test installation of Xubuntu using BackTrack distribution and tools included on it. The thesis is divided into chapters, starting with operating system Linux basics, continuing with requirements for investigator and his equipment to tools used for analysis. All discussed tools are available for free, their size vary from simple and small tools to complex frameworks. Theoretical knowledge is applied to real system and usage of tools is shown. This thesis ends with forensic report, which summarizes all findings gathered during investigation.

Klíčová slova

forenzní analýza, operační systém Linux, distribuce BackTrack, počítačový zločin, digitální důkaz, forenzní vyšetřování, i-uzel, forenzní vyšetřovací prostředí

Keywords

Forensic analysis, Linux operating system, BackTrack distribution, computer crime, digital evidence, forensic investigation, i-node, forensic framework

Citace

Beneš Martin: Forenzná analýza v operačných systémoch Linux, bakalářská práce, Brno, FIT VUT v Brně, 2012

Forenzná analýza v operačných systémoch Linux

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Pavla Očenáška, Ph.D.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Martin Beneš
16. 5. 2012

Poděkování

Chcel by som poďakovať vedúcemu práce pánovi Ing. Pavlovi Očenáškovi, Ph.D. za všetky konzultácie a cenné usmernenia.

Obsah

1 Úvod

Každá ľudská činnosť je v súčasnosti, či už viac alebo menej, zasiahnutá vplyvom informačných technológií. Ich rapídny nárast zapríčinila hlavne klesajúca cena hardware a stále sa zvyšujúca dostupnosť software. Na spoľahlivosť, dostupnosť a bezpečnosť počítačových systémov je kladených čoraz viacej nárokov, pretože spoločnosť sa na nich stáva čoraz viac závislá. Rovnako však narastá aj počet zraniteľností a útokov na ne zameraných.

Tak ako sa počítače stali súčasťou každodenného života, jeho súčasťou sa stal aj počítačový zločin. Počítačové systémy sú v dvoch pozíciách - nástroj zločinu, alebo jeho obeť. Stopy po zločine v týchto systémoch ostávajú, rovnako ako je tomu pri zločine v klasickom zmysle. Tento typ zločinu veľmi často prekračuje hranice jednotlivých štátov. Zároveň definícia toho, čo je a čo nie je legálne, nie je vždy úplne jasná a jednoznačná. Vynucovanie práva je pre spomenutú povahu komplikované. Mechanizmy spolupráce medzi krajinami na riešení a trestaní zločinu sú komplexné a pomalé.

Vyšetrovaním digitálnych dát za cieľom určenia čo, kde a ako sa stalo sa zaoberá práve forenzná analýza. Christopher Brown chápe forenznú analýzu ako umenie a vedu aplikovania znalostí a skúseností počítačovej vedy na pomoc právnemu procesu. [2] Je to proces pri ktorom je potrebné dodržiavať overené postupy a metodológie, ale zároveň zapojiť vlastné myslenie a intuíciu. V širšom zmysle slova, forenzná analýza zahŕňa zber a uchovávanie dôkazových materiálov, ich skúmanie a vyhodnotenie a nakoniec ich dôveryhodné spracovanie v posudku, použiteľnom v právnom procese.

Nasledujúci text sa zaoberá problematikou forenznej analýzy v prostredí operačného systému Linux. Operačný systém Linux bol zvolený pre jeho rozšírenie a pestrosť použitia. Je využívaný na rozličných typoch zariadení, od mobilných telefónov veľkosti ľudskej dlane a jedným procesorom, až po servery zložené z množstva procesorov s neporovnateľnou veľkosťou a výkonom. Dovolím si tvrdiť, že princípy a postupy uvedené v tomto texte, sú s menšími úpravami aplikovateľné aj na iné systémy podobné systému Unix (Unix-like systémy).

2 Operačný systém Linux

Operačný systém (OS) je program, resp. kolekcia programov, ktorá vytvára spojujúcu medzivrstvu medzi hardware výpočtového systému (ktorý môže byť virtualizovaný), užívateľmi a ich aplikačnými programami.[4] Jedným z najviac rozšírených operačných systémov je práve Linux. Tento operačný systém je vyvíjaný komunitou ľudí a žiadna spoločnosť nie je samostatne zodpovedná za jeho vývoj a podporu. Nasledujúce kapitoly popisujú základné princípy operačného systému Linux, potrebné k pochopeniu postupov forenznej analýzy.

2.1 Stručná história OS Linux

Počiatky operačného systému Linux siahajú do roku 1991. V tomto období boli na trhu štyri dominantné operačné systémy. Prvým z nich bol DOS ktorý bol nasadzovaný najmä na osobné počítače a kvôli dômyselnému marketingu sa stále rozširoval. Druhým bol System 7 od firmy Apple, ktorý však kvôli cenovej politike nebol prístupný pre veľké masy ľudí a tak v rozšírenosti zaostával za systémom DOS. Tretím bol systém Unix. Jeho zdrojový kód však nebol voľne dostupný, rozšíreniu neprospievala ani cena. Posledným hráčom bol systém Minix, ktorý vytvoril Andrew S. Tanenbaum na vzdelávacie účely. Zdrojový kód bol voľne dostupný a tak sa začal rozširovať na trhu. Operačný systém Minix nebol dokonalý, ale jeho výhodou bolo to, že každý človek si mohol prečítať jeho zdrojový kód a svojvoľne ho upraviť. Jedným z týchto ľudí bol aj Linus Torvalds.

Začiatkom roku 1991 začal vývoj operačného systému Linux, postaveného na základoch systému Minix. Prvá verzia bola uvoľnená v septembri 1991 a niesla označenie 0.01. Ďalšie verzie nasledovali onedlho. Postupne sa do vývoja zapájali viacerí vývojári a Linux bol uvoľnený pod licenciou GNU General Public Licence. S príchodom grafického užívateľského rozhrania sa operačný systém Linux stal veľmi populárny.

2.2 Súčasnosť

V súčasnosti je systém Linux portovaný na väčšinu bežne rozšírených architektúr. Aj keď pri uvoľnení prvej verzie bol deklarovaný jeho autorom ako hobby, súčasné využitie siaha od malých prenosných zariadení ako sú mobilné telefóny, cez osobné počítače s jedným procesorom až po serverové systémy s tisíckami procesorov. Je šírený pod GNU General Public Licence[1]. Dostupný je v podobe distribúcií (Red Hat, Fedora, Debian, Ubuntu, SUSE, Mandriva, Gentoo a veľa iných).

2.3 Spôsob ukladania dát na disku

Súčasné osobné počítače, ale aj serverové systémy používajú na ukladanie dát záznamové médiá. Súborový systém je systém organizácie dát na disku, ktorý poskytuje procedúry na ukladanie, získavanie a zmenu dát, rovnako ako aj správu voľného miesta na záznamovom médiu. Zvyčajne

[1] http://www.gnu.org/licenses

existuje úzke prepojenie medzi operačným a súborovým systémom. Medzi najpoužívanejšie súborové systémy patria ext2, ext3, ext4, UFS, UFS2, ReiserFS a Reiser4. Vo všetkých spomenutých je použitý koncept tzv. i-uzlu (information node). Obsahu a funkcii i-uzlov bude venovaná samostatná kapitola, pochopenie konceptu je kľúčové pre oblasť forenznej analýzy. V operačnom systéme Linux je skoro všetko považované za súbor, vrátane periférnych zariadení, sieťových kariet, pamätí, adresárov a samozrejme aj súborov. Klasický Linuxový systém súborov pozostáva z:

- Boot bloku
- Super bloku
- Tabuľky i-uzlov
- Dátových blokov

Pričom blok je najmenšia alokovateľná jednotka, jeho minimálna veľkosť je 512 bajtov.

Boot blok obsahuje inštrukcie ktoré zavádzajú operačný systém do pamäti počítača – tzv. zavádzač. V operačnom systéme Linux existuje len jeden boot blok, ktorý sa nachádza na hlavnom pevnom disku.

Super blok obsahuje informácie popisujúce systém (metadáta). Sú v ňom uložené detaily o geometrii disku, dostupnom mieste, umiestnení prvého i-uzlu a ostatných i-uzlov. Obsahuje takisto veľa informácií o konfigurácií daného systému, hlavne veľkosť bloku, názvy súborových systémov a detaily o alokovaných a voľných i-uzloch. Pretože tieto informácie sú nevyhnutné pre správnu funkciu a ich poškodením by sa znehodnotili všetky uložené informácie, býva táto časť na disku uložená viac krát, na rozličných miestach.

Po super bloku nasleduje tabuľka i-uzlov. Táto tabuľka môže byť rozdelená na niekoľko častí. Medzi jednotlivými časťami sa môžu nachádzať dátové bloky. I-uzly sú dynamicky vytvárané a rušené v závislosti na práci so súborovým systémom.

Samotné adresáre a súbory sú uložené v dátovom bloku. Ich poloha je odkazovaná práve z i-uzlov.

2.4 Štart operačného systému

Znalosť procesu zavádzania OS je nevyhnutná pri vykonávaní forenznej analýzy, pretože nie vždy je možné pre získanie dát vypnúť skúmaný systém. Po zapnutí počítača s operačným systémom Linux, je do pamäte nahraný krátky úsek programu, permanentne uloženého v pamäti ROM. Prvou akciou je na väčšine systémov kontrola dôležitých komponentov. Ak prebehne v poriadku, zbernica je testovaná na prítomnosť zariadenia, ktoré obsahuje zavádzací program. Tento program zavedie do pamäti jadro operačného systému (kernel), ktorému je predaná správa ďalších činností. Jadro rozpozná a nakonfiguruje zariadenia a pripraví ich na použite.

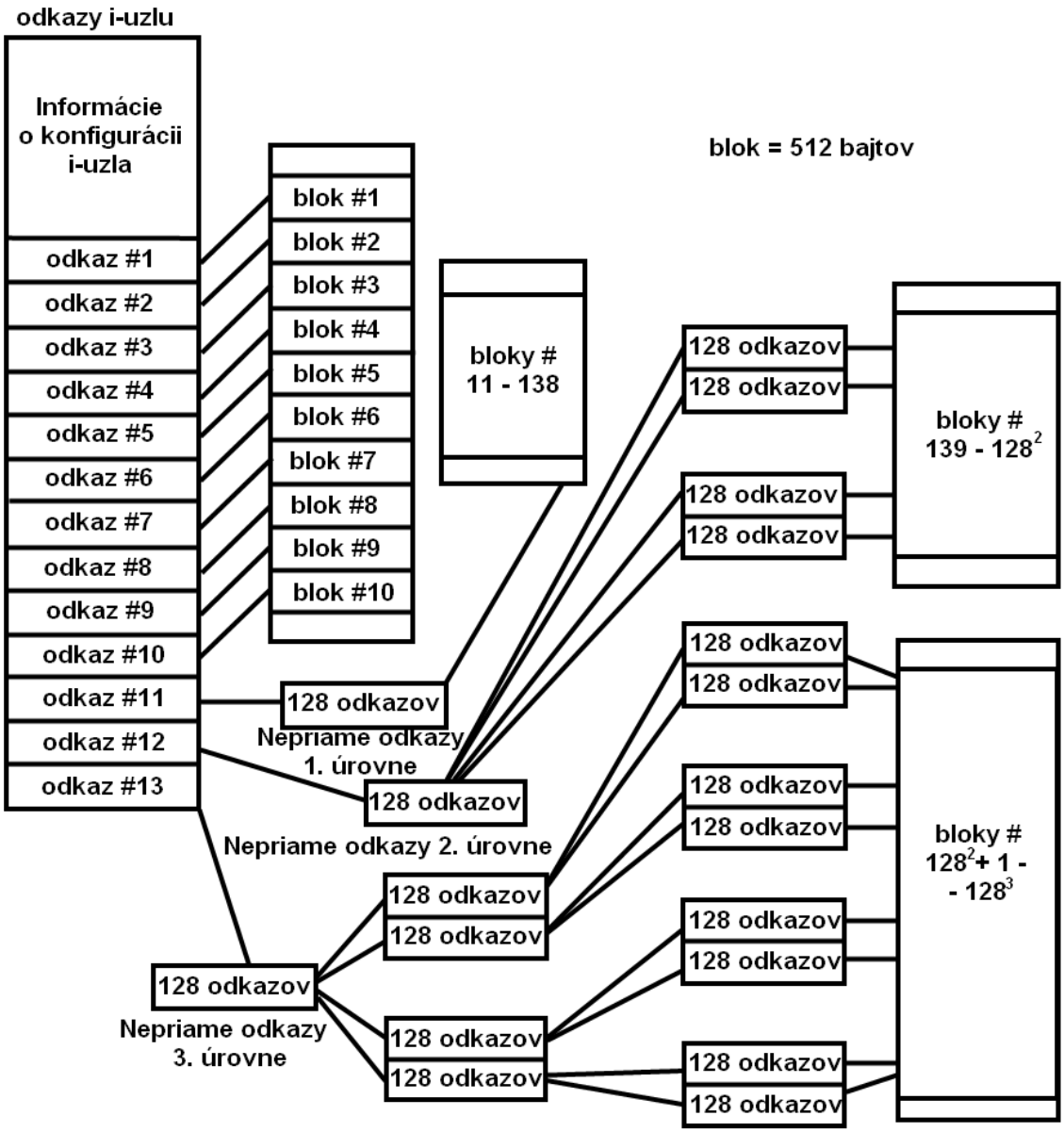
Ak je na fyzickom počítači nainštalovaných viacero operačných systémov, do MBR[2] disku je nainštalovaný tzv. boot manager. Je to krátky program, umožňujúci výber operačného systému, ktorý sa má zaviesť do pamäte. Najviac používané programy sú *Linux Loader (LILO)* a *Grand Unified Boot Loader (GRUB).*

[2] MBR – Master boot record

2.5 I-uzly

I-uzol je základná dátová štruktúra, popisujúca súbor. Poskytuje mechanizmus prepájania dátových blokov. Každý i-uzol obsahuje nasledujúce informácie:

- Stav i-uzlu (alokovaný, voľný)
- Typ súboru (obyčajný, adresár, zariadenie)
- Dĺžka súboru v bytoch
- „mtime“ – čas poslednej modifikácie dát
- „atime“ – čas posledného prístupu
- „ctime“ – čas poslednej modifikácie i-uzlu
- UID – identifikácia vlastníka
- GID – identifikácia skupiny
- Prístupové práva
- Počet pevných odkazov
- Tabuľka odkazov na dátové bloky
- Ďalšie informácie [4]



Obrázok 1: Štruktúra i-uzlu

2.6 Distribúcia BackTrack Linux

Operačný systém Linux vyniká mierou schopnosti prispôsobenia. Je šírený vo forme distribúcií, pričom každú distribúciu je možné klasifikovať ako upravenú pre istý spôsob použitia. Existujú distribúcie vhodné pre bežné použitie, ako pracovné stanice alebo servery, rovnako ako distribúcie pre špecializované použitie. Príkladom sú minimalistické verzie bežiace na špeciálnych zariadeniach (vstavané systémy alebo riadiace jednotky), alebo na bežných zariadeniach, ale so špecializovaným účelom. Predstaviteľom poslednej skupiny je práve linuxová distribúcia BackTrack.

Od svojho počiatku je BackTrack distribúcia určená k penetračnému testovaniu a využívaná úzkou skupinou ľudí, profesionálne sa venujúcim bezpečnosti systémov. Je možné ho nainštalovať na pevný disk, rovnako je však možné systém do pamäti zaviesť z DVD média, alebo USB kľúča. Toto jeho využite rozširuje aj na vykonávanie forenznej analýzy, nehovoriac o vstavanej podpore forenzného vyšetrovania.

Pri výkone forenzného vyšetrovania je nevyhnutné zabezpečiť, aby informácie uložené na zasiahnutom systéme neboli pozmenené pri pokuse o čítanie. Na tento účel boli zo začiatku používané samostatné zariadenia, ktoré umožňovali dáta z média čítať, ale neumožňovali zápis. Nie vždy je však možné podobné zariadenie použiť, preto sa veľmi často používajú programové prostriedky. Live distribúcia Linuxového systému, z ktorej sú odstránené všetky skripty ktoré môžu pozmeniť dáta, je vynikajúci nástroj. BackTrack od verzie 4 podporuje forenzný mód pri zavádzaní systému. V tomto móde nie je zmenený jediný bit cieľového súborového systému, automatické pripojenie dostupných zariadení je vypnuté, časy posledného pripojenia a posledného prístupu k súborom sú zachované a rovnako odkladacie partície nie sú využívané. Postupy a nároky na získanie forenznej kópie dát budú predmetom ďalších kapitol.

BackTrack 5 R2 je v čase písania práce aktuálna verzia tejto distribúcie. Je založená na Ubuntu GNU/Linux[3] verzie 10.04 LTS a zameraná na penetračné testovanie a forenzné vyšetrovanie. Počiatky vývoja tejto distribúcie siahajú do roku 2006, kedy vznikla spojením Auditor Security Linux a distribúcie WHAX[4]. Oproti Ubuntu je rozšírená o zbierku bezpečnostných a forenzných nástrojov. Distribúcia môže byť ľubovoľne upravovaná pomocou balíčkovacieho systému, je jednoduché ju rozšíriť o ďalšie nástroje, aj keď to zvyčajne nie je potrebné. Priamo od vývojového tímu sú dostupné dve základné grafické užívateľské prostredia – Gnome a KDE, samozrejme je možné doinštalovať akékoľvek iné. Existujú dve verzie systému BackTrack – 32 bitová a 64 bitová.

[3] Distribúcia ktorej vývoj zastrešuje spoločnosť Canonical, http://www.ubuntu.com

[4] Vývoj spomenutých distribúcií skončil, alebo skoro vôbec nenapreduje, http://distrowatch.com

3 Forenzná analýza

Okrem viac-menej neformálnej definície forenznej analýzy, ktorú sme spomenuli v úvode sa v dostupnej literatúre vyskytujú aj iné, formálnejšie definície. Jednou z nich je aj nasledujúca formulácia. Forenzná analýza zahŕňa získavanie a analyzovanie digitálnych informácií, za účelom poskytnutia dôkazov civilnému a trestnému právu. [3] Aktivity, pri ktorých sa využíva forenzné vyšetrovanie sú drogová trestná činnosť, nelegálne šírenie digitálneho obsahu, vraždy, detská pornografia, podvody, šírenie škodlivého software, neoprávnené vniknutie do systému a veľa iných závažných trestných činov, alebo porušení interných pravidiel.

3.1 Úvod do forenznej analýzy

Vývoj nových technológií má vždy za následok vývoj vedných disciplín, ktoré danú technológiu skúmajú. Rovnako to je aj s rozšírením informačných technológií. Vyžiadali si vznik veľkého množstva nových vedných odborov. Jedným z nich je aj forenzná analýza. Vedná disciplína forenznej analýzy spočíva v spracovávaní dát z počítačových zdrojov s ohľadom na to, aby výsledky tejto analýzy mohli byť zohľadnené ako právoplatné dôkazy pri súdnom konaní. Ak sa ponoríme viacej do detailov, forenzná analýza zahŕňa bezpečné zbieranie informácií, výber dát ktoré sú v danej situácií zaujímavé, ich analýza zameraná na obsah a pôvod a v konečnom dôsledku prezentácia výsledkov. Nejde iba o informácie uložené na pevnom disku počítača. Predmetom skúmania forenznej analýzy nie sú len samostatné počítače, ale celé počítačové systémy, takže skúma rôzne súčasti týchto systémov vrátane sieťových prvkov, prenosných pamätí, serverových počítačov, osobných počítačov a mobilných zariadení.

Aj keď sa forenzná analýza zaoberá problematikou obnovy dát, nie je vhodné tieto dva pojmy zamieňať. V prípade obnovy dát zvyčajne hľadáme niečo, čo bolo odstránené omylom, alebo nechcene, napríklad počas havárie systému. Vieme teda čo hľadáme a kde to máme hľadať. Prístup v rámci forenznej analýzy je však odlišný. Vo väčšine prípadov vieme čo hľadáme, ale to, kde máme hľadať je neznáme. Naše úsilie môže byť navyše komplikované snahou páchateľa zakryť po sebe stopy.

3.2 História

Vznik forenznej analýzy podmienil rozmach informačných technológií a ich prepojenie s každodenným životom v spoločnosti. Počítačový zločin rastie neustále od 70-tych rokov minulého storočia. V čase vzniku, počítače neboli rozšírené tak ako je tomu dnes, a tak sa ohniská zločinu sústreďovali na sálové počítače, používané v oblasti výskumu, techniky a finančníctva. V tom období to bol pre spoločnosť nový druh zločinu, pre ktorý neexistovali právne postihy. Netrvalo však dlho a legislatíva sa začala vyvíjať.

V 80-tych rokoch sa začali rozširovať osobné počítače. Hlavným rozdielom oproti predchádzajúcemu obdobiu bola cenová dostupnosť počítačov aj pre osobné potreby. Vznikali firmy špecializované na predaj osobných počítačov (Apple, Commodore Business Machines), boli vyvinuté

prvé operačné systémy (PC-DOS, MS-DOS). V tomto období boli založené aj prvé spoločnosti zaoberajúce sa forenznou analýzou. Nástroje na analýzu existovali interne v týchto spoločnostiach, boli jednoduché a nedostupné pre verejnosť. Vznikla prvá asociácia združujúca spoločnosti a jednotlivcov zainteresovaných vo forenznom vyšetrovaní - International Association of Computer Investigative Specialist (IACIS).

S nástupom 90-tych rokov prišlo ešte väčšie rozšírenie osobných počítačov a nástup prvých verejnosti dostupných nástrojov. IACIS dokonca predstavila prvé kurzy forenzného vyšetrovania. Koncom tohto obdobia v komunite odborníkov začal prevládať názor, že proces získavania dôkazov z počítačových systémov by mal byť zjednotený po celom svete a snahy o zjednotenie sú viditeľné dodnes.

Prvá dekáda tohto storočia je spojená s obrovským nárastom výkonu počítačových systémov, rovnako ako aj s rozvojom sietí ktoré tieto systémy prepojujú. Smer vývoja nástrojov určovalo rozšírenie malých osobných zariadení ako napríklad PDA, mobilné telefóny a tablety. Tieto zariadenia rovnako priniesli nové možnosti použitia výpočtových zariadení na porušenie práva.

3.3 Požiadavky forenznej analýzy

Rola osoby alebo tímu, ktorý vykonáva forenznú analýzu, spočíva v zbere dôkazov z podozrivého zariadenia a rozhodnutie, či bol porušený zákon, alebo inak stanovené pravidlá. Je dôležité si uvedomiť, že forenzná analýza nemá svoje uplatnenie len v dokazovaní porušenia zákona, ale môže byť použitá aj na usvedčenie hocijakej inej činnosti. Príkladom je porušenie firemných pravidiel, alebo činnosť ktorá neporušuje zákon priamo, ale je v rozpore s etickým správaním.

V oboch prípadoch však použitie nie je jednoduché a samo môže viesť k narušeniu práva na súkromie. Právny aspekt však presahuje rámec tejto práce, preto je spomenutý len okrajovo. V prípade, že analýza potvrdí incident, je potrebné vytvoriť posudok, ktorý je zozbieraním dôkazov a je možné ho predložiť súdu, alebo inej inštitúcii. Je preto potrebné aby posudok bol vierohodný, nespochybniteľný a v prípade potreby sa dal znovu zrekonštruovať na základe dôkazov. Pre tento účel vznikla metodika postupu, ktorú je dobrým zvykom dodržať.

3.4 Vyhodnotenie rizík

Pri forenznom vyšetrovaní určitého prostredia je nevyhnutná jeho dôkladná znalosť. Len za splnenia tohto predpokladu vyšetrovateľ môže zavčas identifikovať a minimalizovať dopad rizík. Podobne je to aj s voľbou metód forenznej analýzy ktoré budú použité – ich voľba závisí na znalosti systému a použitých technológií.

Proces vyšetrovania je veľmi často komplikovaný snahou páchateľa zakryť po sebe stopy a zničiť každú indíciu, ktorá by viedla k jeho odhaleniu. Existuje viacero techník na skrytie alebo kompletné odstránenie digitálnych informácií a zmätenie vyšetrovateľa.

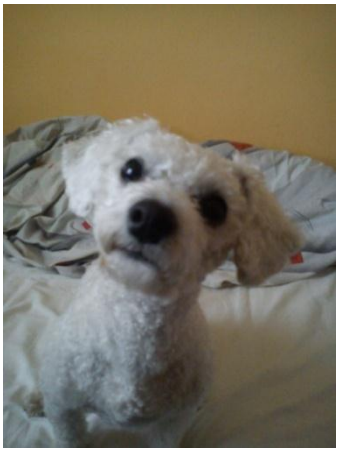
- **Skryté diskové oddiely** – je možné vytvoriť pomocou bežne dostupných programov a nevyžadujú hlboké znalosti princípov uloženia dát na disku. Skryté diskové oddiely nie sú obsiahnuté vo výstupoch štandardných programov a na ich odhalenie je nutný prístup k pamäťovému médiu na nízkej úrovni.

- **Šifrovanie súborového systému –** sa stáva bežne používanou praktikou na súčasných počítačových systémoch. Existuje množstvo šifrovacích algoritmov ktoré je možné využiť. U niektorých z nich sú známe útoky, iné sú doteraz neprelomené. Každopádne šifrovanie veľmi často úplne znemožní, v lepšom prípade len spomalí proces forenzného vyšetrovania snímky disku. U šifrovaných diskových oddielov je dôraz kladený na live analýzu, keďže počas nej je zaručený prístup k dátam. V prostredí operačného systému Linux je najčastejšie používaným nástrojom na šifrovanie celých diskových zväzkov program TrueCrypt[5].
- **Pozmenenie chovania systému –** rôzne formy malware nie sú na platforme Linux rozšírené vo veľkej miere. Ako každý iný systém aj pre tento systém však existujú prelomenia bezpečnosti. Jedným z nich je infekcia rootkitmi. Rootkit je program (kolekcia programov), ktorého hlavnou úlohou je získať plný prístup k počítačovému systému bez autorizácie a vedomia legitímneho vlastníka systému. Cieľom je maskovať vniknutie a získať najvyššiu úroveň prístupu. Na rozdiel od vírusu sa nereprodukuje, ale hlavne sa snaží zakryť svoju existenciu.
- **Steganografia –** je metóda skrývania dát. Pri steganografii je cieľom nielen utajiť obsah správy, ale aj správu samotnú. Ide teda o skrytie prenášanej informácie tak, aby o jej existencii nevedel okrem odosielateľa a prijímateľa nikto iný. V princípe je tajná správa (message) vložená do oveľa väčšieho súboru (carrier) a spracovaná spôsobom špecifickým steganografickému algoritmu tak, aby pozmenený cieľový súbor bol interpretovaný na nerozoznanie od originálneho. Ako nosič sa zvyčajne využívajú mediálne súbory. Sú preferované kvôli svojej bežnosti a rozšírenosti, takže nevzbudzujú dojem že nesú tajnú informáciu. Rovnako sú to typicky veľké súbory, takže sú schopné poňať väčšie množstvo tajnej informácie.

Obrázok 2: Pôvodný (vľavo) a upravený obrázok (vpravo), obsahujúci vstavanú informáciu

Ľavá časť obrázku ukazuje zobrazený pôvodný súbor, použitý ako nosič. Pravá časť vznikla vstavaním obrázku 3 (ktorého existenciu a informačnú hodnotu bolo cieľom zatajiť) do pôvodného súboru. Voľným okom sú obrázky identické.

[5] Voľne dostupný nástroj pre šifrovanie dát na platformách Windows, Mac OS a Linux, špecifikácia dostupná na http://www.truecrypt.org/docs/



Obrázok 3: Súbor vstavaný do obrázku slnečníc

V tomto prípade bola ukrytá len neškodná fotografia môjho psa. V iných prípadoch však môžu byť ukryté závažné dôkazy (detská pornografia, odcudzené priemyselné vzory, plány budov...).

- **Spôsob mazania súborov –** V operačných systémoch Linux je rušenie súborov zaistené volaním *unlink*. Pri mazaní súboru odstráni pevný odkaz medzi menom súboru a i-uzlom. Systém udržuje informáciu o počte procesov, ktoré používajú daný súbor. Ak počet mien a počet procesov ktoré používajú súbor klesne na nulu, i-uzol a bloky ktoré súbor zaberal sú uvoľnené. [1] Znalosť princípu činnosti systému pri rušení súboru umožňuje použitie pokročilých techník na obnovu súborov.

3.5 Metodický postup

Ako už bolo spomenuté, forenzná analýza je veda ktorá vznikla nedávno a vyvíja sa postupne. Teoretické postupy a systematický prístup dlhú dobu podliehali snahám o zjednotenie. V súčasnosti je základná metodológia ustálená, jej hlavné prvky v nasledujúcej kapitole sú prevzaté z literatúry. [3]

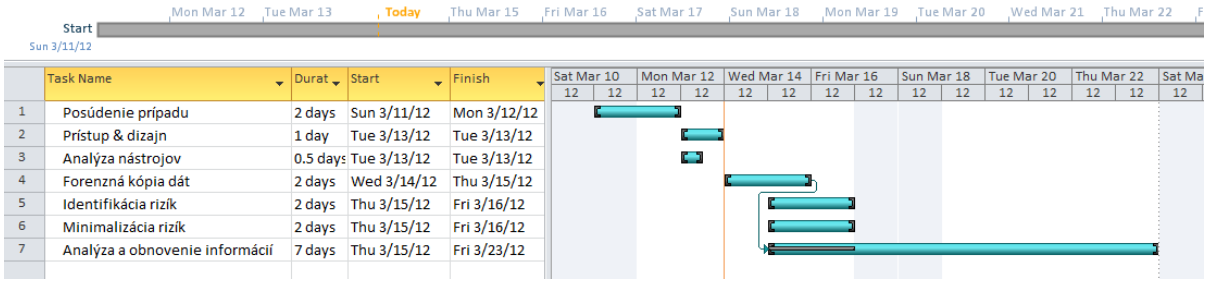
- **Prvotné posúdenie prípadu**
  Spočíva v oboznámení sa s prípadom, okolnosťami ktoré nastali, prostredím v ktorom sa incident odohral a osobami ktoré boli zahrnuté. V tejto fáze je dôležité rozhodnúť či bol počítač použitý na spáchanie zločinu, alebo iba obsahuje dôkazy o incidente.

  Dôležitou súčasťou je posúdenie okolia. Rovnako ako v iných (klasických) formách zločinu, každý jeden detail môže zohrať významnú úlohu v tom, či výsledok vyšetrovania bude správny, alebo nie. Zanedbanie, alebo nechcené znehodnotenie dôkazov môže narušiť dôveryhodnosť posudku ako celku. Preto je vhodné vykonať dokumentáciu prostredia (fotografie, audio a video nahrávky).

- **Voľba prístupu k incidentu a dizajnu štúdie**
  Aby celkový prístup k analýze nebol náhodný a mal vnútornú logiku, je potrebné zvoliť hlavné kroky hneď na začiatku. Výstup tohto kroku nie je detailným plánom analýzy, ale je jednoduchou osnovou akcií v chronologickom poradí.

  Je potrebné zamerať pozornosť na systematický prístup k procesu analýzy. Nie všetky už vykonané kroky je možné vrátiť do stavu v ktorom krok začínal, čo môže priniesť neprekonateľné prekážky. Tieto riziká je treba poznať vopred a včas sa vyhnúť chybám.
- **Vytvorenie detailného zoznamu akcií**
  V tomto štádiu je osnova z predchádzajúceho kroku doplnená o kroky, ktoré sú zrozumiteľné a je možné jasne určiť mieru ich splnenia. Analýza prípadu je dlho trvajúca akcia, preto je vhodné, nie však nevyhnutné, každý krok doplniť odhadovanou dĺžkou trvania. Takto je možné sledovať skutočný postup voči odhadovanému a operatívne meniť plán ak to situácia vyžaduje.

  Pri vyšetrovaní prípadu je veľmi často nevyhnutné reportovať dosiahnuté výsledky a fázu vyšetrovania. Existuje viacero prístupov k plánovaniu projektov. Jedným z často využívaných je Ganttov graf. Je to stĺpcový graf ktorý zobrazuje plán a súčasný stav projektu. Ilustruje začiatočné a koncové časy úloh. Úlohy na sebe môžu byť závislé a môžu mať medzi sebou vzťahy.



- **Určenie potrebných nástrojov**
  Nástroje potrebné na vykonanie analýzy závisia na type úlohy. Hlavným faktorom určujúcim výber je dostupnosť nástrojov pre dané prostredie. Výber ovplyvňuje najmä typ zariadenia a operačný systém ktorý na zariadení beží. Pre rôzne úlohy existujú špecifické nástroje a svoju úlohu zohrávajú aj osobné preferencie a skúsenosti.

  Existujú dva typy nástrojov – programové a hardwarové. Svoju úlohu pri vyšetrovaní samozrejme zohráva aj rozpočet vyčlenený pre potreby vyšetrovateľa. Popri operačnom systéme a type úlohy, práve rozpočet najviac ovplyvňuje výber nástrojov; existujú špecializované hardwarové nástroje s vysokou zriaďovacou cenou, komerčne vyvíjané programové nástroje, ale aj voľne šíriteľné nástroje. Téme voľne dostupných nástrojov je venovaná samostatná kapitola.
- **Získanie kópie dát z napadnutého systému**
  Vytvorenie forenznej kópie disku, zvyčajne pomocou špecializovaných nástrojov. Požiadavky na kópiu budú analyzované neskôr.
- **Identifikácia rizík**
  Detailné zváženie rizík a situácií, ktoré môžu nastať. Obsahuje riziká vyplývajúce z podstaty operácií, ale aj situácie, ktoré mohli byť vytvorené úmyselne, v snahe zabrániť získaniu citlivých dát zo systému.

Z bezpečnostného hľadiska je nevyhnutné myslieť o krok dopredu. Páchateľ sa rovnako ako pri klasikom zločine vždy snaží zakryť za sebou stopy a čím viac zneistiť vyšetrovateľa. V systéme môžu existovať nástrahy, ktoré je nutné predvídať.

- **Minimalizácia rizík**
  Tento krok nadväzuje na zoznam definovaný v predchádzajúcom kroku. Je samozrejmé, že našim cieľom je úplná minimalizácia rizík. Nie vždy je to však možné či už technicky, alebo tým že do identifikácie rizík nezahrnieme situáciu ktorá môže nastať.
- **Testovanie dizajnu**
  Pred samotnou analýzou je potrebné uistiť sa o správnosti krokov, ktoré boli vykonané doteraz. Analýza je komplexný proces a počas postupu sa môžu vyskytnúť problémy, ktoré sa v raných štádiách nevyskytovali. Rovnako prebieha verifikácia vzorky dát ktorú máme k dispozícii, napríklad pomocou kontrolných súčtov a hashovacích funkcií. Cieľom je overenie korešpondencie pôvodných dát a kópie.

  Osvedčenou praktikou sa stala verifikácia plánu druhou osobou. Nie vždy je táto možnosť k dispozícii, ale zvyčajne vnesie kritický pohľad. Do prípadu nezasvätená osoba prinesie nové nápady a rovnako môže prispieť k eliminácii rizík.
- **Analýza a obnovenie informácií**
  Analýza a obnovenie informácií je hlavnou časťou procesu. Cieľom je vyhľadanie právnym procesom akceptovateľných dôkazov. Používame nástroje a kópiu dát získanú v predchádzajúcich krokoch, postupujúc podľa detailného plánu, snažiac sa minimalizovať riziká. Rovnako aj tejto téme je venovaná samostatná kapitola.
- **Vytvorenie forenzného posudku**
  Výsledky analýzy sú popísané v záverečnej správe – forenznom posudku. Správa musí byť kompletným popisom všetkých akcií ktoré boli vykonané a nálezov ktoré boli objavené. Vytvára sa v štandardizovanom formáte, s prihliadnutím na povahu daného prípadu.
- **Zhodnotenie prípadu**
  Tento bod nie je priamo vo vzťahu s forenznou analýzou, slúži skorej na rozvoj osobných schopností a je prípravou na nasledujúce vyšetrovanie. Po ukončení prípadu je vhodné vyhodnotiť vykonané kroky a posúdiť ich opodstatnenosť a prínos.

4 Nástroje forenznej analýzy

Kvalita a kvantita forenzných nástrojov rástla so zložitosťou a rozšírením informačných technológií. V súčasnosti používané nástroje analýzy sú buď jednoduché nástroje, zvyčajne zamerané na jednu špecifickú činnosť, alebo sú to softwarové balíky ktoré zvládajú komplexné činnosti. Ako v každej oblasti, aj v tejto existujú komerčné nástroje a nástroje, ktoré sú dostupné voľne, zvyčajne pod licenciou GNU GPL. V tejto kapitole sa zameriame na voľne dostupné nástroje, keďže tieto budú použité aj v neskorších kapitolách.

4.1 Rozdelenie nástrojov

Nástroje je možné klasifikovať podľa fázy forenznej analýzy, v ktorej sú nasadené. Väčšina je zahrnutá v hlavnom nástroji ktorý bude pre analýzu použitý – distribúcia OS Linux špecializovaná na penetračné testy a forenznú analýzu – BackTrack. Podľa tejto klasifikácie rozlišujeme nástroje pre:

- Zber dát
- Verifikáciu dát
- Obnovu dát
- Analýza metadát
- Sieťovú analýzu
- Analýzu logovacích súborov
- Reportovanie výsledkov a evidencia dôkazov

4.2 Vyšetrovacie nástroje

Na rozdiel od forenznej analýzy v operačných systémoch Windows majú vyšetrovacie nástroje do istej miery štandardizované rozhranie. Dokumentácia je ľahko dostupná, a to v manuálových stránkach. Pre účely vyšetrovania existujú samostatné špecializované nástroje, ale nemalú úlohu hrajú aj bežne používané programy.

4.2.1 GNU core utilities

GNU core utilities, skrátene *coreutils* [5] je kolekcia základných programov pre manipuláciu s textom a súbormi v operačných systémoch. Programy obsiahnuté v tejto kolekcii sa zvyčajne nachádzajú v každom Unix-like systéme. Projekt vznikol v roku 2002, spojením troch kolekcií (*fileutils*, *shellutils* a *textutils*) do jednej. Hoci nasledujúce nástroje nepatria priamo medzi forenzné nástroje, v linuxovom prostredí sú veľmi často využívané.

- ***cat*** – kopíruje každý súbor na vstupe (štandardný vstup, ak nie je špecifikovaný iný) na štandardný výstup. Najčastejšie sa používa na zobrazenie obsahu textových súborov. S využitím prepínačov je možné rozšíriť funkcionalitu (číslovanie riadkov a podobne)

- ***head*** **–** vytlačí začiatok súboru (predvolený počet riadkov je 10) na štandardný výstup. Pri niektorých súboroch sú pre analýzu potrebné informácie skryté práve v hlavičke súboru. Zbytok obsahu nie je dôležitý a jeho čítanie z disku môže byť vynechané. Chovanie programu je ovplyvnené argumentmi. Jednou z často používaných modifikácií je zmena počtu čítaných riadkov na počet bajtov. Podobne ako tento nástroj funguje program ***tail***, ktorý zobrazí koniec súboru.
- ***wc*** **–** spočíta bajty, znaky, slová a riadky v zadaných súboroch. Ak je zadaných viacero súborov, program počíta aj sumu hodnôt. V rámci predvoleného správania program vytlačí počet riadkov, slov a bajtov, iné správanie je vyvolané zadaním dodatočných argumentov.
- ***md5sum*** **–** spočíta 128 bitový md5 kontrolný súčet všetkých súborov ktoré dostane. Súčty sú počítané podľa RFC 1321[6]. Aj keď bolo dokázané že md5 súčty môžu produkovať kolízie, tento program sa stále používa na verifikáciu dát. Je možné počítať kontrolný súčet z textového súboru, rovnako ako z binárnych súborov.
- ***sha1sum*** **–** je program využitím podobný predchádzajúcemu, avšak kontrolný súčet počíta pomocou algoritmu SHA1[7]. Produkuje 160 bitový výstup. Jeho použitie je podobné programu *md5sum*. Algoritmus SHA2[8] využívajú podobné programy: ***sha224sum***, ***sha256sum***, ***sha384sum*** a ***sha512sum*** s dĺžkou výstupu 224, 256, 384 a 512 bitov.
- ***ls*** **–** program vypíše informácie o súboroch. Pre argumenty, ktoré sú adresármi vypíše obsah daného adresáru, pričom predvolene nepostupuje rekurzívne a vynecháva súbory začínajúce znakom „.“. Pre argumenty ktoré nie sú adresármi, vypíše len meno súboru. Ak nie je zadaný argument, vypíše sa obsah aktuálneho adresára. V predvolenom chovaní je výstup zoradený abecedne, s prihliadnutím na lokálne nastavenie. Pri forenznej analýze sa využíva možnosť výpisu skrytých súborov, čiže tých, ktorých názov začína znakom –„.“. Často sa používa dlhý formát výpisu a možnosť zoradenia podľa času modifikácie.
- ***cp*** **–** kopíruje súbor. Program skopíruje súbor zadaný prvým argumentom do súboru zadaného druhým argumentom. Správanie programu závisí na type vstupných argumentov, adresáre nie sú v predvolenom režime kopírované, ale v rekurzívnom režime sú adresáre aj vytvárané.
- ***dd*** **–** kopíruje súbor, pričom môže vykonávať konverziu. Ovládanie programu sa odlišuje od ostatných nástrojov tejto skupiny, chovanie je ovplyvnené pomocou operandov. Typickými operandami sú if=file, of=file, ibs=bytes, bs=bytes,count=blocks . Tento nástroj je používaný pri vytváraní bitových kópií.
- ***mv*** **–** presunie alebo premenuje súbor. Akýkoľvek typ súboru (obyčajný súbor, symbolický link, rúra) môže byť prenesený z jedného súborového systému na iný.
- ***rm*** **–** odstráni súbor. V predvolenom móde nedokáže odstrániť adresár. Ak je súbor odstránený pomocou programu rm, za normálnych podmienok je možné ho znovu obnoviť. Tohto javu často využíva práve forenzná analýza.

[6] Dokument dostupný na http://www.ietf.org/rfc/rfc1321.txt

[7] Dokument dostupný na http://www.ietf.org/rfc/rfc3174.txt

[8] Dokument dostupný na http://www.ietf.org/rfc/rfc5754.txt

- ***rmdir*** **–** odstráni prázdny adresár. Nie je možné použiť na adresár ktorý nie je prázdny, v tom prípade je nutné využiť program *rm* s parametrom zaisťujúcim rekurzívne správanie.
- ***touch*** **–** zmení čas prístupu alebo modifikácie súboru. Ak nie je zadané inak, časová značka je nastavená na aktuálny čas. Ak súbor so zadaným menom neexistuje, je vytvorený nový. Štandardná cesta vytvorenia nového súboru je práve pomocou príkazu *touch*.
- ***df*** **–** výpis použitého a voľného miesta na súborových systémoch. Často používaný je parameter zaisťujúci prevod počtu bajtov na pre ľudí čitateľnejší formát.
- ***stat*** **–** zobrazí informácie o zadanom súbore. Bez parametrov zobrazí všetky informácie o súbore dodanom ako argument.
- ***pwd*** **–** na výstup vytlačí cestu k aktuálnemu adresáru
- ***who*** **–** poskytuje cenné informácie o tom, kto je práve prihlásený k systému. V prípade vzdialeného prístupu vypíše aj IP adresu alebo doménové meno odkiaľ sa užívateľ prihlasuje.
- ***date*** **–** zobrazenie aktuálneho dátumu a času linuxového systému.

4.2.2 Nástroje používané na zber materiálu

Získavanie dát je počiatočnou fázou analýzy. Spočíva v získavaní identickej kópie disku a analyzovaní bez zanechania stôp na originálnom systéme. Hlavnými zástupcami tejto kategórie sú unixová utilita *dd* a program *aimage*. Vytvára tzv. bitovú kópiu dát. Ďalšími predstaviteľmi sú *dcfl*, *RDA*, a *afflib* (balík nástrojov).

4.2.3 Detekcia programov typu rootkit

Infekcia systému rootkitmi je pre forenzné vyšetrovanie nebezpečná a je nutné, aby bola odhalená v ranom štádiu vyšetrovania, keďže dokáže ovplyvniť činnosť iných programov používaných na analýzu. Najčastejšie používané nástroje na detekciu sú chkrootkit a rkhunter, oba sú obsiahnuté v distribúcií BackTrack.

- ***chkrootkit*** **–** je skript, ktorý je schopný detekcie modifikácie binárnych súborov za účelom zneužitia. Bez zadania dodatočných parametrov kontroluje binárne súbory operačného systému ktorý práve beží. Keďže napadnuté môžu byť aj programy ktoré pre svoj beh používa samotný skript, pri spustení sa zadáva alternatívna cesta k systémovým programom (napríklad na pripojenom disku, flash pamäti). Pri spustení z bezpečného systému sa vhodným zadaním argumentov dá vynútiť kontrola pripojeného disku, častejšie využívanou metódou je však zmena koreňového adresára skriptu na prípojný bod, kde je pripojený disk.
- ***rkhunter*** **–** je nástroj na monitorovanie a analýzu bezpečnosti systémov spĺňajúcich štandard POSIX, ktorý pomáha s detekciou rootkitov, malware a dokáže vykonať automatizovanú kontrolu bezpečnosti systému. Výstup programu obsahuje veľké množstvo výstrah, ktoré nie sú aktuálnou hrozbou (tzv. false positive alarmy). Kontrola preto nie je plne automatizovaná, ale je nutná validácia výsledkov.

4.2.4 Správa dát na nízkej úrovni

- ***hexedit*** **–** existuje viacero programov s rovnakým názvom, my sa však zameriame na nástroj obsiahnutý v distribúcií BackTrack. Hexedit slúži na zobrazenie a editáciu súborov v ASCII alebo hexadecimálnom zobrazení. Je vhodný pri prehľadávaní obsahu súborov, zobrazovaní metadát na úrovni nižšej ako sú samotné dáta. Silnou stránkou je možnosť čítať zariadenie (device) ako súbor. Vlastnú implementáciu programu hexedit obsahuje každé komplexné prostredie určené na forenznú analýzu a nízkoúrovňový prístup k súborom.

4.2.5 Analýza súborov a diskových snímok

- ***bulk_extractor*** **–** je nástroj vyvíjaný v jazyku C++, za účelom získavania informácií zo snímok diskov súborových systémov. Vďaka zanedbaniu štruktúry súborového systému dokáže spracovanie dát paralelizovať, čím dosahuje vyššiu rýchlosť spracovania. Program vyhľadáva informácie o číslach kreditných kariet, doménové mená, vrátane IP adries a MAC adries, emailové adresy, EXIF dáta z JPEG obrázkov a videí, telefónne čísla, URL, detaily o zip archívoch a veľa iných užitočných informácií.
- ***exif-tool*** **–** EXIF[9] dáta sú súčasťou väčšiny rozšírených grafických súborových formátov. Informácie do nich vkladajú digitálne fotoaparáty, kamery, ale aj mobilné telefóny a iné zariadenia ktoré dokážu vytvárať digitálne snímky. Pre forenzné vyšetrovanie majú tieto informácie nemalý význam, keďže okrem iného obsahujú výrobcu a model zariadenia ktorým bola snímka vytvorená, dátum a čas vytvorenia a u niektorých zariadení dokonca zemepisné súradnice miesta vytvorenia snímky. Prácu s EXIF informáciami umožňuje práve exif-tool, ktorý disponuje širokou paletou podpory súborových formátov. Vyvinutý je v jazyku Perl a nezávislý na platforme.
- ***stegdetect*** **–** nástroj na vyhľadávanie stenografických informácií v obrázkoch. Dokáže rozpoznať obrázky spracované viacerými stenografickými metódami. Vyvinutý v rámci balíka OutGuess, hlavným vývojárom je Niels Provos. Beží na viacerých platformách, podporuje však len obrázky typu jpeg.

4.2.6 Extrakcia dát

Rovnako ako v prípade klasického zločinu je bežné, že páchateľ za sebou zakryje stopy. Do úvahy prichádzajú dve situácie, páchateľ zmaže súbor, alebo ho prepíše inými dátami, čo je horšia možnosť (za tretiu možnosť treba považovať neúmyselné prepísanie zmazaného súboru operačným systémom).

- ***extundelete*** **–** nástroj slúžiaci na obnovu súborov na oddieloch so súborovým systémom ext3 alebo ext4. Program využíva informácie uložené v žurnále na obnovu súborov zmazaných z oddielu. Je možné nastaviť obnovu jediného súboru, ale aj všetkých súborov na celom diskovom oddiele.

[9] Štandard pre ukladanie metadát v obrazových súboroch, súčasť štandardu DCF, vytvoreného asociáciou JEITA (www.jeita.or.pl)

- ***foremost*** – najpoužívanejší nástroj na extrakciu dát, dokáže extrahovať dáta na základe pokročilých vlastností ako sú hlavičky, päty a štruktúra súboru. Keďže pri behu neberie ohľad na obsah tabuliek súborového systému, nerozlišuje medzi existujúcimi a zmazanými súbormi. Obsahuje vstavané predefinované šablóny, ale funkcionalita môže byť rozšírená vlastnými štruktúrami. Definícia hlavičky a päty sa nachádza v konfiguračnom súbore foremost.conf. Jeho editáciou je možné pridať ďalšie detekované súbory podľa potreby.

```
#               case    size    header                  footer
#extension   sensitive
#-----------------------------------------------------------------
# PNG   (used in web pages)
#       (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
#       png     y       200000  \x50\x4e\x47?   \xff\xfc\xfd\xfe
#
# BMP
#       (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
#       bmp     y       100000  BM??\x00\x00\x00
#
# AVI (Windows animation and DiVX/MPEG-4 movies)
#       (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
#       avi     y       4000000 RIFF????AVI
#
# Word documents
#       (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
#       doc     y       12500000  \xd0\xcf\x11\xe0\xa1\xb1
#
#MISCELLANEOUS
#       zip     y       10000000   PK\x03\x04      \x3c\xac
#       (NOTE THIS FORMAT HAS BUILTIN EXTRACTION FUNCTION)
#       rar     y       10000000        Rar!
```

- ***magicrescue*** – je nástroj s funkciou podobnou programu *foremost*. Vo svojej podstate prehľadá blokové zariadenie a obnoví súbory kontrolovaním magického čísla. Zariadenie sa otvára len na čítanie, súbory sú extrahované pomocou externých programov.
- ***safecopy*** – nie je vyslovene nástroj forenzného vyšetrovania, využitie nájde skorej ako nástroj na záchranu dát z fyzicky poškodených zariadení. Avšak aj pri forenznom vyšetrovaní nastávajú situácie, v ktorých je vyšetrovateľ nútený k záchrane dát z poškodeného média aj za cenu straty dát. *Safecopy* na rozdiel od ostatných nástrojov v kategórii číta tak veľa dát, ako je len možné. Iné nástroje zastavia čítanie ako náhle narazia na poškodenú oblasť, ale *safecopy* pokračuje a preskakuje len poškodené bloky.
- ***scalpel*** – známy nástroj umožňujúci definovanie databázy štruktúr súborov a následné vyhľadávanie. Pomocou konfiguračného súboru (podobnému súboru programu *foremost*) je možné definovať, ktoré typy súborov potrebujeme získať zo zariadenia.
- ***ddrescue*** – kopíruje dáta z jedného súboru alebo blokového zariadenia na druhé snažiac sa zachrániť dáta ak sa vyskytne pri čítaní chyba. Tento program je vhodné využiť ak existujú dve alebo viacej poškodených kópií súboru. Ak nad nimi spustíme program ddrescue s jedným výstupným súborom, pravdepodobne dostaneme pôvodný súbor bez chýb. Pravdepodobnosť poškodenia súborov na rovnakom mieste je veľmi nízka.

4.2.7 Sieťová analýza

Nástroje sieťovej analýzy sú špecifické tým, že hlavné využitie je mimo oblasti forenznej analýzy. Sú vyvíjané hlavne pre potreby správy sietí a penetračného testovania. Ich vlastnosti však umožňujú aj nasadenie vo forenznej analýze. Navrhnuté boli na zachytenie komunikácie, jej uloženie a následnú možnosť spracovania. Keďže pôvodnou funkciou distribúcie BackTrack bolo práve penetračné testovanie, táto oblasť je najviac prepracovaná. Z nástrojov spomenieme *tcpdump, kismet* a samozrejme najrozšírenejší nástroj – *wireshark.*

4.2.8 Kontrola integrity

Jedným zo základných nárokov na forenzné vyšetrovanie je možnosť overenia, že forenzná kópia dát sa zhoduje s originálnym systémom. Bežný postup je vytvorenie hashov obidvoch systémov a ich následné porovnanie. V prípade zhody môžeme vyhlásiť forenznú kópiu za zhodnú so súborovým systémom ktorý je vyšetrovaný.

Na vytvorenie hashu distribúcii BackTrack obsahuje balík nástrojov s názvom hashdeep. Programy obsiahnuté v balíku počítajú MD5, SHA-1, SHA-256, Tiger a Whirlpool hashe. Programy sú veľmi podobné nástrojom z balíka coreutils, ich pridaná hodnota je v rozšírenej funkcionalite. Dokážu fungovať rekurzívne, odhadnúť očakávanú dobu výpočtu, počítať hash po častiach, alebo len pre špecifické súbory.

4.2.9 Digital forensics framework

Dff je nástoj, ktorý podľa jeho vývojárov vznikol ako reakcia na neexistenciu kvalitného, voľne dostupného prostredia na forenzné vyšetrovanie. Pomenovanie vzniklo skrátením z Digital Forensics Framework. Zdrojový kód je napísaný v jazykoch C++ a Python, balík sa vyznačuje svojou modulárnou architektúrou poskytujúcu výkon a rozšíriteľnosť. Dff pozostáva z nástrojov, knižníc, modulov a užívateľského rozhrania. Základnou funkciou je zhromažďovanie informácií a analýza zväzkov, súborových systémov a dát v nich obsiahnutých. Základné vlastnosti sú:

- **Open source –** zdrojový kód je šírený pod licenciou GNU/GPL. Prístup k zdrojovým kódom umožňuje úpravu software podľa vlastných požiadaviek. Nástroj je spravovaný komunitou vývojárov a nie je viazaný na konkrétnu spoločnosť.
- **Prenositeľnosť –** samotné prostredie aj nástroje ktoré využíva sú dostupné vo všetkých populárnych operačných systémoch.
- **Skiptovateľnosť –** prostredie poskytuje vysokú mieru automatizácie pomocou profilov a vlastných skriptov.
- **Modularita –** dizajn prostredia je objektovo orientovaný. Keďže oba jazyky v ktorých bol napísaný sú objektovo orientované, umožňuje rozšírenie pomocou modulov napísaných v C++ a Python.
- **API –** rozhranie pre programovanie aplikácií – na rozdiel od komerčných prostredí, dff disponuje rozhraním, ktoré umožňuje vývoj vlastných aplikácií. Rozhranie je prístupné pomocou kolekcie objektovo orientovaných knižníc, ktoré poskytujú prístup k funkcionalite potrebnej na vykonávanie forenznej analýzy.

4.2.10 PTK forensics

Ptk je komplexná zbierka nástrojov a rozširujúcich modulov slúžiacich na analýzu médií. Grafické užívateľské rozhranie je realizované webovým rozhraním, využíva štruktúru LAMP[10]. Je grafickou nadstavbou nad nástrojmi balíka The Sleuthkit. Ptk je jedným z mála nástrojov, ktorý nie je udržovaný komunitou vývojárov, ale je vyvíjaný spoločnosťou DFlabs. Nekomerčné použitie je však bezplatné, podmienené registráciou. Prostredie ptk podporuje užívateľské účty, umožňuje personalizáciu pomocou používateľských profilov. Vlastnosti určujúce použitie ptk sú:

- webová aplikácia s centralizovanou databázou
- podpora všetkých rozšírených prehliadačov
- logovanie všetkých operácií
- ptk je obmedzené na použitie v operačnom systéme Linux
- ako centrálne úložisko používa databázu MySql
- rozhranie vytvára Apache server s PHP5

4.2.11 Autopsy

Autopsy je svojou podstatou podobné prostrediu *ptk*, tiež je to grafické užívateľské rozhranie, operujúce nad nástrojmi balíka sleuthkit. Funguje na princípe klient-server, kedy serverová časť je reprezentovaná webovým serverom a klienti sa pripájajú zo svojich vlastných systémov. Architektúra umožňuje prácu viacerých vyšetrovateľov na jednom serveri. Špecializuje sa na analýzu diskových oddielov alebo snímok. Súborové systémy ktoré môžu byť týmto nástrojom spracované sú NTFS, FAT, UFS1, UFS2, ext2 a ext3. Na rozdiel od *ptk* je prostredie šírené pod voľnou licenciou GPL2 a je možné ho používať aj pod operačným systémom Windows (s pomocou Cygwin[11]). Je možné použitie v dvoch situáciách:

- **Analýza spusteného systému –** kedy analyzuje systém počas jeho behu (live analýza). V tomto prípade je *Autopsy* spustené z odoberateľného média v prostredí ktorému nie je možné dôverovať. Táto možnosť nie je preferovaná, keďže programy môžu byť pozmenené, čo môže ovplyvniť výsledky analýzy. Analýza spusteného systému sa vykonáva počas prvej reakcie na incident, poprípade ak neexistuje iná možnosť (vypnutie systému by malo vážne následky).
- **Analýza vypnutého systému –** je vykonávaná v dôveryhodnom prostredí, zvyčajne vo forenznom laboratóriu alebo na nezmenenej, čistej inštalácií systému. Keďže všetky programy majú očakávané správanie a prostredie je dôveryhodné, táto možnosť je preferovaná pred analýzou spusteného systému. Je však nevyhnutné brať do úvahy že vypnutím systému môže prísť k strate niektorých dát.

[10] Linux-Apache-MySql-PHP – kombinácia operačného systému, webového servera, SQL databáze a programovacieho jazyka PHP

[11] Kolekcia software, poskytujúca štandardné Unix/Linux prostredie v systémoch Windows (http://www.cygwin.com)

Autopsy vyniká možnosťou správy prípadov. Pre analýzu každého jedného systému je možné vytvoriť samostatný prípad v ktorom sú uložené všetky informácie a výsledky. Vyšetrovania sú triedené podľa prípadov, ktoré obsahujú jeden alebo viacero systémov. Každý systém má nastavenú svoju časovú zónu a môže obsahovať jeden alebo viac snímok disku. Časovú následnosť akcií vykonaných v rámci vyšetrovania definujú udalosti. Obsahujú časový odtlačok, takže môžu byť radené a prehľadne zobrazené v sekvenciách. Pre možnosť spolupráce viacerých vyšetrovateľov sú k dispozícii poznámky, ktoré je možno pridávať jednotlivým vyšetrovateľom alebo systémom. Systém všetky vykonané akcie loguje, pre možnosť spätne dohľadať čo ktorý vyšetrovateľ vykonal. Hashe, ktoré zaručujú že snímky diskov neboli pozmenené sú počítané automaticky, ale je možné integritu skontrolovať aj na základe požiadavku od vyšetrovateľa.

4.2.12 The Sleuthkit

The Sleuthkit (*TSK*) je zbierka nástrojov na forenznú analýzu, ktorá vznikla ako nástupca *The Coroner's toolkit*[12] prostredia. *The Sleuthkit* je knižnica jazyka C a kolekcia programov spustiteľných v príkazovom riadku. Niektoré obsiahnuté programy sú podobné štandardným programom z balíka *coreutils*, ale keďže sú zamerané na forenzné vyšetrovanie, nie sú ignorované skryté a zmazané súbory. TSK dokáže:

- Analyzovať bitové kópie diskov (*dd*) ale aj kópie vytvorené inými forenznými programami – *Encase* a *afflib*
- Podporuje NTFS, FAT, UFS1, UFS2, Ext2, Ext3, HFS a ISO9660 systémy
- V prípade NTFS zväzkov zobraziť súbor a všetky jeho atribúty
- Vyhľadávať hashe podozrivých súborov v on-line databázach
- Organizovať súbory na základe ich typu
- Bežať na všetkých populárnych operačných systémoch – Linux, Mac OS X, FreeBSD, Solaris a Windows.

[12] Predchodca TSK, vývoj prostredia bol ukončený (http://www.porcupine.org/forensics/tct.html)

5 Praktický postup

Samotná forenzná analýza digitálneho obsahu sa skladá z troch hlavných častí, pričom každá časť je zložená z ďalších špecifických úloh. Prvou z častí je príprava dát. Začína získaním kópie dôkazového materiálu, následnou extrakciou informácií, identifikáciou potencionálne zaujímavých súborov a plynule prechádza do druhej fázy, ktorou je analýza dát. Táto časť je jadrom forenznej analýzy a spočíva vo vyhľadávaní informácií, ktoré je možné použiť ako dôkazný materiál. Informácie získané v druhej časti sú spracované v poslednej fáze – vo forenznom posudku. Cieľom je vytvorenie správy ktorá, detailne popisuje vykonané kroky a závery z nich vyvodené. Správa musí byť písaná s ohľadom na čitateľa (súd, zamestnávateľ, zadávateľ projektu), jasná a zrozumiteľná cieľovej skupine. [1]

5.1 Zaistenie dôkazov

Forenzné vyšetrovanie začína vždy na mieste kde sa incident odohral. Platia podobné pravidlá ako pri klasickom zločine, cieľom je nezničiť a neznehodnotiť dôkaznú hodnotu materiálu. Základným princípom je nepozmeniť dôkazný materiál, zabrániť útočníkovi aby znovu získal prístup do systému, zálohovať dôkazný materiál a dokumentovať všetky vykonané akcie. Dôkazný materiál (väčšinou vo forme záznamového média) musí byť uložený v prostredí kde nie je ovplyvnený javmi, ktoré by ho mohli znehodnotiť. Patrí sem najmä silné elektromagnetické pole, prach a statická elektrina. Nasleduje dokumentácia okolia zasiahnutého systému. Miesto činu musí byť dôkladne zdokumentované pre možnú rekonštrukciu v budúcnosti. Dokumentácia obsahuje fotografie, náčrtky a videozáznam miesta a okolností. Dôraz je kladený na polohu systému a periférne zariadenia ktoré sú k nemu pripojené (klávesnica, externá pamäť, tlačiareň a podobne). Ak je pripojené zobrazovacie zariadenie, v dokumentácií je zobrazený aktuálny stav. Na základe získaných faktov a ďalších informácií je pre ďalší postup nutné rozhodnúť sa, či je nutné vypnúť systém a pokračovať vo vyšetrovaní z dôveryhodného prostredia, alebo bude spustená tzv. live analýza, kedy sú nástroje spúšťané z vymeniteľného média alebo sieťovej lokality. Často krát nastáva situácia, kedy je dostupná len analýza spusteného systému, pretože jeho vypnutie nie je z rôznych dôvodov možné. Ak je systém vypnutý, toto rozhodovanie odpadá a systém znova nezapíname. Naopak, ak je zapnutý, odpojenie od elektrickej siete a batérií je spôsob vypnutia, ktorý zanechá systém v neporušenom stave. Nie vždy je však táto metóda bezpečná, preto sme nútení vypnúť systém klasickým spôsobom. Hrozí však riziko straty a pozmenenia dôkazov.

5.2 Live analýza

Je metódou získavania nestálych dát z vyšetrovaného systému. Nie vždy je možné ju vykonať z dôvodu straty dát, ale ak je riziko pozmenenia dát nízke, je prvotnou reakciou na incident. Medzi nestále dáta patria napríklad bežiace procesy, otvorené sieťové sokety a obsah pamäti, čiže informácie, ktoré sú pri vypnutí systému nenávratne stratené.

5.2.1 Vytvorenie dôveryhodného prostredia

Pri analýze zapnutého systému nie je možné dôverovať informáciám získaným z prostredia operačného systému. Každý jeden program môže byť pozmenený tak, aby zakryl isté informácie. Riešením tohto problému je spustenie potrebných nástrojov z dôveryhodnej lokality, ako je pripojené vymeniteľné médium alebo sieťové umiestnenie. Nástroje takto pripojené k systému musia byť preložené pre cieľovú architektúru. Použijeme USB kľúč, vopred naformátovaný súborovým systémom ext3 na ktorý sme v distribúcií BackTrack nahrali požadované nástroje. Osvedčeným postupom je premenovanie nástrojov, aby neboli omylom zamenené za nedôveryhodné.

Preferovanou možnosťou je vykonanie live analýzy z lokálneho príkazového riadku, keďže páchateľ stále môže monitorovať sieťovú komunikáciu. Prístup s právami užívateľa root je nevyhnutný.

Z výstupu programu fdisk vidíme, že pripojený USB kľúč bol v systéme identifikovaný ako zariadenie */dev/sdb*. Obsahuje jediný diskový oddiel, ktorým je */dev/sdb1*.

```
root@test-srv:~# fdisk -l

<detaily pevného disku sú vynechané>

Disk /dev/sdb: 4023 MB, 4023386112 bytes
17 heads, 48 sectors/track, 9630 cylinders, total 7858176 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000c6460

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1            2048     7858175     3928064   83  Linux
root@test-srv:~#
```

Aby bolo možné pristupovať na USB kľúč, je nutné ho najprv pripojiť k systému využitím nástroja mount. Pri live analýze je snahou zamedziť akémukoľvek zápisu na disk, preto všetky získané informácie budú ukladané na USB kľúč. Z toho vyplýva potreba pripojenia v režime umožňujúcom zápis. USB kľúč pripojíme do podadresára adresára */media*, ktorý je určený na pripojovanie súborových systémov.

```
root@test-srv:~# mkdir /media/usb
root@test-srv:~# mount -o rw /dev/sdb1 /media/usb
root@test-srv:~# cd /media/usb/
root@test-srv:/media/usb# ls
lost+found  tools
root@test-srv:/media/usb#
```

V adresári *tools* sa nachádzajú pripravené nástroje premenované pridaním prefixu „t“ (trusted). Ako prvý spustíme dôveryhodný príkazový riadok a pokračujeme získavaním informácií pomocou ostatných nástrojov.

```
root@test-srv:/media/usb# cd tools/
root@test-srv:/media/usb/tools# ls -al
total 2140
drwxr-xr-x 2 root root   4096 2012-05-06 12:13 .
drwxr-xr-x 4 root root   4096 2012-05-06 12:13 ..
-rwxr-xr-x 1 root root 818232 2012-05-06 12:13 tbash
-rwxr-xr-x 1 root root  50836 2012-05-06 12:13 tchmod
-rwxr-xr-x 1 root root  54964 2012-05-06 12:13 tchown
-rwxr-xr-x 1 root root  96140 2012-05-06 12:13 tcp
-rwxr-xr-x 1 root root  63128 2012-05-06 12:13 tdate
-rwxr-xr-x 1 root root  54996 2012-05-06 12:13 tdd
-rwxr-xr-x 1 root root  67316 2012-05-06 12:13 tdf
-rwxr-xr-x 1 root root  30212 2012-05-06 12:13 techo
-rwxr-xr-x 1 root root 100372 2012-05-06 12:13 tgrep
-rwxr-xr-x 1 root root  13776 2012-05-06 12:13 tlast
-rwxr-xr-x 1 root root   9696 2012-05-06 12:13 tlastlog
-rwxr-xr-x 1 root root 104528 2012-05-06 12:13 tls
-rwxr-xr-x 1 root root 129504 2012-05-06 12:13 tlsof
-rwxr-xr-x 1 root root  38508 2012-05-06 12:13 tmd5sum
-rwxr-xr-x 1 root root  30372 2012-05-06 12:13 tmore
-rwxr-xr-x 1 root root  87944 2012-05-06 12:13 tmv
-rwxr-xr-x 1 root root 110088 2012-05-06 12:13 tnetstat
-rwxr-xr-x 1 root root  75600 2012-05-06 12:13 tps
-rwxr-xr-x 1 root root  54928 2012-05-06 12:13 trm
-rwxr-xr-x 1 root root  13824 2012-05-06 12:13 tscript
-rwxr-xr-x 1 root root  55364 2012-05-06 12:13 tsed
-rwxr-xr-x 1 root root  13844 2012-05-06 12:13 tw
root@test-srv:/media/usb/tools# cd
root@test-srv:~# /media/usb/tools/tbash
root@test-srv:~#
```

5.2.2 Zaznamenanie aktuálneho stavu systému

Niektoré, pre forenzné vyšetrovanie nenahraditeľné informácie nie je možné získať z vypnutého systému. Práve ich získanie je cieľom live analýzy. Prvou informáciou ktorá umožní správne chronologické usporiadanie udalostí je zistenie aktuálneho času afektovaného systému a dopočítanie časového posunu k reálnemu času.

```
root@test-srv:~# /media/usb/tools/tdate
Sun May  6 12:45:01 CEST 2012
root@test-srv:~#
```

Na zhromažďovanie získaných informácií o systéme vytvoríme na USB kľúči adresár *evidence* do ktorého budeme ukladať získané dôkazy. Výstupy programov môžu byť uložené do súboru použitím štandardného presmerovania.

```
root@test-srv:~# mkdir /media/usb/evidence
root@test-srv:~# /media/usb/tools/tdate > /media/usb/evidence/date
root@test-srv:~#
```

Predmetom forenzného vyšetrovania veľmi často bývajú serverové systémy, kde je v jednom čase pripojených veľa užívateľov. Na dokumentáciu prihlásených používateľov slúži program *w*.

```
root@test-srv:~# /media/usb/tools/tw
 14:07:55 up  3:45,  2 users,  load average: 0.08, 0.15, 0.12
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
benny    pts/0    192.168.1.11     12:31   17.00s  0.64s  0.00s -bash
root       pts/2      localhost            14:07      0.00s   0.50s   0.00s
/media/usb/tools/tw
root@test-srv:~#
```

Súbory v operačných systémoch Linux obsahujú tri časové odtlačky. Je to čas prístupu (atime), modifikácie obsahu súboru (mtime) a čas zmeny vlastnosti i-uzlu (ctime). Tieto časové otlačky je možné získať pomocou nástroja *ls* a rovnako ich uložiť na USB kľúč.

```
root@test-srv:~# /media/usb/tools/tls -altRu / >
/media/usb/evidence/access_times
root@test-srv:~# /media/usb/tools/tls -altRc / >
/media/usb/evidence/change_times
root@test-srv:~# /media/usb/tools/tls -altR / >
/media/usb/evidence/modify_times
```

Ďalším krokom je overenie sieťových spojení a otvorených soketov. Štandardným nástrojom je program *netstat*.

```
root@test-srv:~# /media/usb/tools/tnetstat -all
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:www                   *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp             0       224  test-srv.local:ssh          192.168.1.11:1145
ESTABLISHED
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 *:36804                 *:*
udp        0      0 *:mdns                  *:*
udp6       0      0 [::]:50836              [::]:*
udp6       0      0 [::]:mdns               [::]:*
```

Z prvých troch riadkov výpisu vidíme, že daný systém prijíma spojenia na portoch pre www (port 80 je otvorený v dôsledku aktívneho webového serveru) ssh (port 22 je používaný ssh serverom) a ipp (631 predvolene povolený port pre Internet printing protocol). Nasledujúci riadok ukazuje nadviazané vzdialené ssh spojenie k počítaču s IP adresou 192.168.1.11. Keďže systém podporuje IPv6, prijíma spojenia aj na IP adresu protokolu IPv6 (s výnimkou webového serveru, pretože podpora v ňom nie je zapnutá). Posledné štyri riadky však nie je možné identifikovať na prvý pohľad, preto spustíme nástroj netstat s inými parametrami, aby sme identifikovali aplikácie ktoré využívajú otvorené porty.

```
root@test-srv:~# /media/usb/tools/tnetstat -ulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address    Foreign Address   PID/Program name
udp        0      0 *:36804          *:*               649/avahi-daemon: r
udp        0      0 *:mdns           *:*               649/avahi-daemon: r
udp6       0      0 [::]:50836       [::]:*            649/avahi-daemon: r
udp6       0      0 [::]:mdns        [::]:*            649/avahi-daemon: r
root@test-srv:~#
```

Odkiaľ môžeme usúdiť že porty sú oprávnene používané systémom Avahi[13]. Kompletný zoznam otvorených portov s priradenými aplikáciami uložíme na USB kľúč.

```
root@test-srv:~# /media/usb/tools/tnetstat -anp >
/media/usb/evidence/open_ports
root@test-srv:~#
```

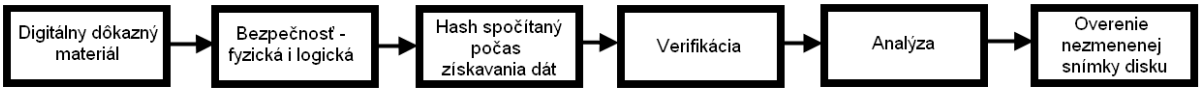
Pokračujeme záznamom a kontrolou bežiacich procesov. Na toto použitie je ideálny nástroj *ps* (process status).

```
root@test-srv:~# /media/usb/tools/tps aux > /media/usb/evidence/ps_out
root@test-srv:~# head -5 /media/usb/evidence/ps_out
USER  PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root    1  0.0  0.0   3316  1788 ?        Ss   10:22   0:00 /sbin/init
root    2  0.0  0.0      0     0 ?        S    10:22   0:00 [kthreadd]
root    3  0.0  0.0      0     0 ?        S    10:22   0:01 [ksoftirqd/0]
root    6  0.0  0.0      0     0 ?        S    10:22   0:00 [migration/0]
root@test-srv:~#
```

Z výstupu vidíme kto proces spustil a rovnako aj kedy začal, čo je užitočná informácia ak vieme približný čas kedy sa incident odohral.

5.3 Získanie forenznej kópie dát

Cieľom tohto kroku je získanie informácií zo zasiahnutého systému, ale bez akéhokoľvek pozmenenia pôvodných dôkazov, ktoré musia ostať neporušené od získania až po ukončenie právneho procesu, ba dokonca dlhšie kvôli archivácií dôkazov. Zameráme sa na statické získavanie dát z vypnutého systému. S nástupom novších operačných systémov sa čoraz častejšie zavádza šifrovanie celého systémového disku. V takomto prípade je možné dáta získať len zo zapnutého systému. V tejto práci však nepredpokladáme šifrované médium. Fáza získavania dát sa na rozdiel od predchádzajúcej už nemusí odohrávať na mieste činu. Zvyčajným miestom je forenzné laboratórium. Z originálu dôkazového materiálu sa pomocou hashovacích funkcií spočíta digitálny odtlačok, vytvorí sa jedna alebo viacero bitových kópií a ich digitálny odtlačok sa porovná s pôvodným odtlačkom. Nasledujúce kroky priamo závisia na tomto kroku, z čoho vyplýva že integrita dát je nutná pre správne výsledky forenznej analýzy. Dôkazový materiál musí byť skúmaný spôsobom, ktorý zaručí fyzickú a logickú bezpečnosť a zachovanie integrity dát. Najčastejšie používanou metódou overenia



Obrázok 4: Proces forenznej analýzy

je porovnanie digitálnych otlačkov hashovacích funkcií. Hashovacia funkcia vygeneruje na základe algoritmu odtlačok. Ten je úplne odlišný ak dôjde k zmene dát, čiže zmena je viditeľná ihneď. Súbežne s tvorbou snímku disku originálneho média je spočítaný aj hash dát na disku. Verifikačný hash je vytvorený nad snímkou disku až po ukončení získavania dát, ale ešte predtým než je snímka

[13] Systém vyhľadávania služieb pomocou balíka protokolov mDNS/DNS-SD, špecifikácia dostupná na http://avahi.org/

analyzovaná. Zhodou oboch hashov je zaručená integrita dát – počas získavania forenznej kópie disku nedošlo k zmene dát. Záverom vyšetrovania je vhodné znovu vygenerovať hash na overenie toho, že snímka nebola počas spracovania pozmenená. Rovnako takto overená kópia môže byť znovu použitá, ak si to vyžaduje ďalšie vyšetrovanie. [7]

5.3.1 Ochrana disku voči zápisu

Operačné systémy Windows sa automaticky snažia pripojiť každý objavený diskový oddiel. Týmto sú bez možnosti obnovenia stratené nenahraditeľne potrebné informácie, ako napríklad čas posledného pripojenia a súbory v dočasných adresároch. Aj keď operačný systém Linux sa takto vo svojej podstate nespráva, môže mať nakonfigurované isté skripty, ktoré automaticky pripoja každý rozpoznaný diskový oddiel. Na ochranu voči nechcenému zápisu existujú dva typy ochrany. Hardwarová ochrana spočíva v pridaní zariadenia blokujúceho zápis na médium. Zariadenia tohto druhu sú bežne dostupné na trhu. Naopak softwarová ochrana nepotrebuje žiadnu ďalšiu investíciu. Bežne sa používa Live CD/USB so systémom Linux, nakonfigurovaným tak, aby diskové oddiely nepripájal automaticky. Niektoré programy dokážu blokovať zápis na ešte nižšej úrovni. Nástroj *PDBlock*[14] mení obsluhu prerušenia INT 13H v BIOSe[15], čím efektívne blokuje každý zápis na periférne zariadenie.

5.3.2 Formát uloženia digitálneho dôkazného materiálu

Existuje veľké množstvo formátov, ktoré sú schopné uchovávať forenzné kópie diskov. Komerčné programy používané na účely analýzy zvyčajne majú svoje vlastné formáty, ktoré sú viac-menej podporované aj v iných nástrojoch. V každom komerčnom programe však nájdeme podporu pre dva open-source formáty:

raw formát – je bitová kópia disku alebo súboru. V minulosti sa kópie vykonávali zo zasiahnutého disku na disk rovnakej veľkosti alebo väčší. Moderné operačné systémy však prišli s možnosťou skopírovať obsah celého disku do súboru. Kopírovanie je rýchle, schopné opravy malých chýb pri čítaní. Nevýhodou je nemožnosť kompresie dát, výstupný súbor potrebuje toľko miesta, ako bola veľkosť kopírovanej jednotky. Tento formát je výstupným formátom nástroja *dd* z balíka *coreutils*. Použitie programu *dd* je jednoduché a rýchle, bohužiaľ má aj svoje nevýhody. Automaticky neopakuje čítanie nad poškodenými sektormi, do cieľového súboru nezachytáva dôležité informácie (sériové číslo disku, čas kedy bola akvizícia dát vykonaná) a je veľmi jednoduché zničiť kopírované dáta zadaním nesprávnych argumentov. Spustenie programu *dd* a vytvorenie kópie diskového oddielu vyzerá takto:

```
root@bt:~# dd if=/dev/sdb of=image conv=noerror,sync
9762816+0 records in
9762816+0 records out
4998561792 bytes (5.0 GB) copied, 468.731 s, 10.7 MB/s
root@bt:~#
```

[14] Komerčný forenzný nástroj dostupný na http://www.digitalintelligence.com/software/disoftware/pdblock/

[15] Basic Input Output System, prvý kód ktorý je spustený pri štarte počítača

formát AFF – vznikol skrátením Advanced Forensics Format a bol vyvinutý Simsonom Garfinkelom v rámci projektu *AFFLIB*[16]. Je to rozšíriteľný otvorený formát ktorý môže byť použitý na viacero účelov, pričom jeho primárnym účelom je ukladanie forenzných kópií diskov. Dizajn formátu AFF je rozdelený na dve vrstvy:

- disc-representation vrstva – ktorá definuje schéma použité pre uloženie štruktúry snímku a metadáta s ňou spojené
- data-storage vrstva – ktorá špecifikuje ako sú segmenty uložené v cieľovom súbore.

Na vytvorenie forenznej kópie s formátom AFF sa najčastejšie používa nástroj *aimage* (ktorý zvláda aj výstup do raw formátu). AFF podporuje kompresiu dát dvomi algoritmami – zlib a LZMA [8]. Program aimage nie je obsiahnutý v distribúcií BackTrack, ale je možné ho doinštalovať pomocou štandardného balíčkovacieho systému. Program je značne užívateľsky prívetivejší ako dd. Počas svojho behu zobrazuje viacej informácií, čo umožňuje pokročilé plánovanie postupu.

```
root@bt:~# aimage -b /dev/sda5 ~/snap/xubuntu.aff
im->outfile=/root/snap/xubuntu.aff
*****************************                  IMAGING                  REPORT
*****************************
Input: /dev/sda5
  Model: WDC_WD1200BEVS-07LAT0  S/N: WD-WXE107596079
  Output file: /root/snap/xubuntu.aff
  Bytes read: 4,998,561,792
  Bytes written: 2,376,651,898

raw image md5:  D7CD E9BB 0829 10E0 CAB4 EAC8 889B 995A
raw image sha1: 23BD 1DD6 41A9 2C22 A057 9933 7EB9 D110 D664 8C4B
raw image sha256: A7B9 D416 5522 00A2 C99E 68A0 AA3C 4B12 3C1D 6EAB 9A39
5164 E931 2EA5 76CF DC43
*** IMAGE WAS VERIFIED ***
Free space remaining on capture drive:  14,627 MB
root@bt:~#
```

Keďže program bol dizajnovaný na vytváranie forenzných kópií, je to poznať aj na jeho správaní. Spustením s vhodnými parametrami je možné docieliť automatickej verifikácie, ako to vidíme na výstupe vyššie. Neoceniteľnou vlastnosťou je možnosť kompresie dát, ktorou je možné dosiahnuť kópií, ktoré zaberajú oveľa menej priestoru. Obidva súbory na nasledujúcom výstupe sú forenznými kópiami rovnakého diskového oddielu. Pri použití AFF formátu je oproti bitovej kópii vytvorenej programom *dd* badať viac ako 50% úsporu miesta!

```
root@bt:~/snap# ls -lh
total 6.9G
-rw-r--r-- 1 root root 2.3G 2012-04-30 22:16 xubuntu.aff
-rw-r--r-- 1 root root 4.7G 2012-04-30 21:21 xubuntu.img
root@bt:~/snap#
```

5.4 Verifikácia získaných kópií

Získavanie forenznej kópie disku je časovo náročné, hlavne pri neustále sa zvyšujúcich kapacitách pevných diskov. Ak je už snímka disku kompletná, overíme že forenzná kópia je zhodná s dôkazným

[16] Open Source Computer Forensics Software, http://afflib.org

materiálom. Najpoužívanejším spôsobom overenia je využitie štandardných nástrojov z balíka coreutils. Dokážu spočítať hash rovnako pre súbory ako aj pre celé diskové oddiely:

```
root@bt:~# md5sum /dev/sda5
b7d90fdd0924cae8ce2d191d224f074f  /dev/sda5
root@bt:~# sha1sum /dev/sda5
7f3abfe5fedb533158d97eb2ea26ba215b037f17  /dev/sda5
root@bt:~#
```

Nástroje balíka hashdeep majú rozšírenú funkcionalitu, dokážu rozpoznať aká časť vstupu je už spracovaná a porovnaním s celkovou veľkosťou odhadnúť čas, ktorý je potrebný na úplne spočítanie hashu.

```
root@bt:~# md5deep -e snap/xubuntu.img
/root/snap/xubuntu.img 1048MB of 4767MB done, 00:02:25 left
b7d90fdd0924cae8ce2d191d224f074f  /root/snap/xubuntu.img
root@bt:~# sha1deep -e snap/xubuntu.img
/root/snap/xubuntu.img 2031MB of 4767MB done, 00:01:30 left
7f3abfe5fedb533158d97eb2ea26ba215b037f17  /root/snap/xubuntu.img
root@bt:~#
```

5.5 Extrakcia dát

Pod pojmom extrakcia dát rozumieme obnovenie dát z kópií, ktoré boli odobrané na mieste činu. Rozlišujeme dve fázy extrakcie dát. Pri fyzickej extrakcii sú obnovené dáta bez ohľadu na súborový systém. Na druhej strane logická fáza identifikuje a obnovuje súbory a dáta na základe inštalovaného operačného systému, súborového systému alebo aplikácií. [9]

5.5.1 Extrakcia na fyzickej úrovni

Zanedbanie štruktúry súborového systému pri fyzickej extrakcii umožňuje vyhľadávanie kľúčových slov, alebo reťazcov určitého formátu, obnovu súborov ktoré nie sú nijako spojené s operačným systémom a skúmanie tabuľky s rozdelením disku. Nástrojom ktorý zanedbanie štruktúry využíva na svoj beh je *bulk_extractor*. Prehľadáva celý diskový oddiel a do výstupných súborov ukladá reťazce odpovedajúce rôznym vzorom (IP adresa, e-mailová adresa, číslo kreditnej karty, EXIF informácie a podobne).

```
root@bt:~# bulk_extractor -j 5 -o ~/out ~/snap/xubuntu.img
bulk_extractor version:1.2.0
Hostname: bt
Input file: /root/snap/xubuntu.img
Output directory: /root/out
Disk Size: 4998561792
Threads: 5
Phase 1.
15:56:41 Offset 0MB (0.00%) Done in n/a at 15:56:40
15:56:42 Offset 16MB (0.34%) Done in  0:07:14 at 16:03:56
15:56:42 Offset 33MB (0.67%) Done in  0:05:26 at 16:02:08

<<hlásenia o postupe sú vynechané>>

root@bt:~#
```

Užitočnou vlastnosťou je hlavne automatické vytváranie textových histogramov pre domény, emailové adresy a telefónne čísla. Prvé priečky histogramu síce obsadzujú domény a emailové adresy zozbierané z manuálových stránok, avšak po vyfiltrovaní zaujímavých adries je možné vytvoriť štatistiky s vysokou informačnou hodnotou.

5.5.2 Extrakcia na logickej úrovni

Logická extrakcia má pridanú hodnotu v tom, že vstup neberie len ako prúd dát, ale k extrakcii používa informácie zo súborového systému, čiže rozlišuje súbory a adresáre. Tým je predurčená na úkony ako extrakcia súborov jedného typu (na základe prípony súboru alebo hlavičky), obnovenie zmazaných súborov, získanie informácií z práve nepoužitého priestoru disku a samozrejme získanie prehľadu o adresárovej štruktúre, súboroch a ich vlastnostiach.

Aj keď distribúcie Linuxu sú si navzájom podobné, v spôsobe rozloženia dát do adresárovej štruktúry existujú rozdiely. Dodržujú síce určité konvencie čo ktorý adresár obsahuje, je však len na používateľovi či ich dodrží alebo nie. Linuxové systémy sú navyše veľmi prispôsobivé a môžu byť rozdelené na viacero diskových oddielov, ba dokonca aj diskov a fyzických systémov. Systém môže byť nakonfigurovaný tak, že adresár */bin, /root* a */boot* sú na jednom disku a jednom oddiele, adresár */var* je na inom oddiele toho istého disku, adresár */tmp* je na inom disku a adresár */home* je pripojený ako sieťová jednotka a nachádza sa na úplne inom fyzickom systéme.

Zobrazenie prípojných bodov je prehľadné použitím nástroja *df*. Keďže rozdelenie na viacero diskov je bežné skorej na serverových systémoch, na ilustráciu slúži výstup tohto programu získaný na školskom serveri merlin.fit.vutbr.cz.

```
xbenes02@merlin: ~$ df | head -12
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda2             32779340   3662200  27452004  12% /
none                  16543336       148  16543188   1% /dev/shm
/dev/sda3             66861996  14750964  52111032  23% /root
/dev/sda4            190654640   3189748 187464892   2% /tmp
/dev/sdb2            437407232 155840284 281566948  36% /usr/local
/dev/sdc2             66861996  39446032  27415964  59% /var
/dev/sdd2            290954944 104435116 186519828  36% /pub
eva:/home/users     4864992944 2470198320 2005595200  56% /homes/eva
eva:/var/mail        145925904  46760416  87491408  35% /homes/mail
kazi:/home/users    9734511552 2556648848 6399101792  29% /homes/kazi
minerva1:/mnt/data  21474705408 18533467136 2941238272  87% /mnt/minerva1
xbenes02@merlin: ~$
```

Prvým krokom k získaniu prístupu k forenznej kópií dát je pripojenie kópie k systému, na ktorom vykonávame forenzné vyšetrovanie. Linux obsahuje natívnu podporu tzv. loopback zariadení. Jeho účelom je simulovať klasické zariadenie, čím umožňuje pripojenie súboru ako disku a jeho následné použitie bez akéhokoľvek obmedzenia. [10] Aby bola zaručená neporušenosť kópie, pripojuje sa v režime read-only. Pripomeniem, že kópia bola vytvorená nástrojom *dd* a proces popísaný v predchádzajúcej kapitole.

```
root@bt:/# mkdir /media/disk
root@bt:/# mount -t ext3 -o ro,loop ~/snap/xubuntu.img /media/disk/
root@bt:/#
```

Odteraz je forenzná kópia dát pripojená do adresára */media/disk* a môžeme s ňou pracovať. V prípade že už pripojenie nie je potrebné nástroj *umount* súbor odpojí.

```
root@bt:~# umount /media/disk/
root@bt:~#
```

Overenie pripojenia v režime read-only je jednoduché. Pri pokuse o vytvorenie súboru operačný systém hlási chybu.

```
root@bt:/# cd /media/disk/
root@bt:/media/disk# touch TESTFILE
touch: cannot touch `TESTFILE': Read-only file system
root@bt:/media/disk#
```

5.5.3 Zoznam súborov

V počiatku logickej extrakcie je preto nutné získať obraz o rozdelení dôležitých adresárov. Na tento účel sú vhodné štandardné linuxové nástroje.

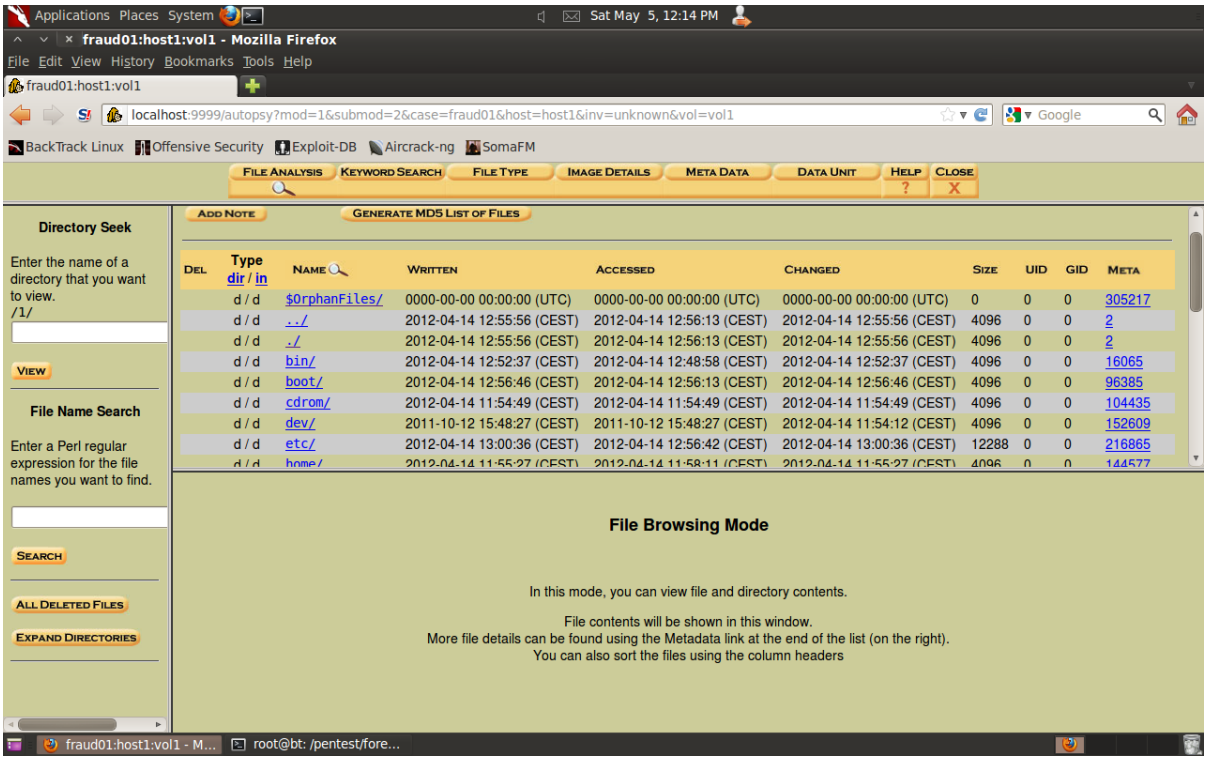
Program *ls* zobrazí obsah aktuálneho adresára. V prípade že sa práve nachádzame v koreňovom adresári, výstup vyzerá na väčšine linuxový systémov podobne:

```
root@bt:/media/disk# ls
bin   cdrom  etc   initrd.img      lib         media  opt   root  sbin
srv  tmp  var      vmlinuz.old
boot  dev    home  initrd.img.old  lost+found  mnt    proc  run   selinux
sys  usr  vmlinuz
root@bt:/media/disk#
```

Získanie prehľadu o celkovej adresárovej štruktúre je možné použitím programu *du*. Jeho výstup je značne obsiahly, pretože vypíše rekurzívne celú adresárovú štruktúru systému. Zvyčajne sa preto jeho výstup limituje, alebo používa v adresároch s malým počtom podadresárov.

```
root@bt:/media/disk# du | head -10
4       ./root/.pulse
20      ./root
4       ./home/benny/Desktop
4       ./home/benny/Documents
52      ./home/benny/.cache/oneconf/8d03b4f13d2289fab5a2a3d300000005
56      ./home/benny/.cache/oneconf
4       ./home/benny/.cache/dconf
8       ./home/benny/.cache/sso
12      ./home/benny/.cache/update-manager-core
4       ./home/benny/.cache/sessions
root@bt:/media/disk#
```

Použitím vyššie spomenutých nástrojov dokáže adresárovú štruktúru užívateľsky príjemnejšie zobraziť nástroj *Autopsy*. Ak už poznáme štruktúru súborového systému disku, môžeme prejsť k špecifickým metódam získavania informácií.



Obrázok 5: Adresárová štruktúra forenznej kópie v programe Autopsy

5.5.4 Extrakcia zmazaných súborov

Najčastejšou technikou ktorou sa páchateľ snaží zakryť stopy alebo zničiť dôkazy je zmazanie súboru. Súbory často bývajú mazané používateľmi bez toho, aby čo i len pomysleli na to, že obsah sa dá veľmi ľahko obnoviť pomocou špecializovaných nástrojov.

Pri plánovaní obnovy dát zohráva dôležitú úlohu súborový systém z ktorého budú dáta obnovené. Každý systém má svoje špecifiká, či už použitie žurnálu alebo spôsob uloženia dát na disku, preto neexistuje program, ktorý zvládne obnovu dát zo všetkých súborových systémov.

Podpora obnovy dát zo súborového systému ext2 nie je obsiahnutá v distribúcii BackTrack. Je to spôsobené tým, že systém ext2 je pomaly vytlačovaný modernejšími súborovými systémami. Pre obnovenie dát z tohto typu systému je potrebné zo systémových repozitárov doinštalovať napríklad program *e2undel*. Keďže na ext2 oddiele môže byť veľké množstvo zmazaných súborov, nástroj ich rozdelí do časových intervalov podľa toho kedy boli zmazané. Interval je nutné vybrať podľa času kedy sa odohral incident, ktorý podnietil forenznú analýzu.

```
root@bt:~# e2undel -a -t -d /dev/sdb1 -s /root/recovered
e2undel 0.82
Trying to recover files on /dev/sdb1, saving them on /root/recovered

/dev/sdb1 opened for read-only access
/dev/sdb1 was not cleanly unmounted.
Do you want wo continue (y/n)? y
245760 inodes (245743 free)
982134 blocks of 4096 bytes (964384 free)
last mounted on Thu Jan  1 01:00:00 1970

/dev/sdb1 is mounted. Do you want to continue (y/n)? y

reading log file: opening log file: No such file or directory
no entries for /dev/sdb1 in log file
searching for deleted inodes on /dev/sdb1:
|==================================================|
245760 inodes scanned, 4 deleted files found

   user name | 1 <12 h | 2 <48 h | 3  <7 d | 4 <30 d | 5  <1 y | 6 older
-------------+---------+---------+---------+---------+---------+--------
        root |       4 |       0 |       0 |       0 |       0 |       0
Select user name from table or press enter to exit: root
Select time interval (1 to 6) or press enter to exit: 1

  inode     size  deleted at        name
-------------------------------------------------------------
     12      165  May  5 15:05 2012 * ASCII text
     13      410  May  5 15:05 2012 * ASCII text
 196609        0  May  5 15:05 2012 * empty
 196610   215952  May  5 15:05 2012 * image/x-png
Select an inode listed above or press enter to go back: 12
165 bytes written to /root/recovered/inode-12-ASCII_text
Select an inode listed above or press enter to go back: 13
410 bytes written to /root/recovered/inode-13-ASCII_text
Select an inode listed above or press enter to go back: 196610
215952 bytes written to /root/recovered/inode-196610-image_x-png
Select an inode listed above or press enter to go back:

   user name | 1 <12 h | 2 <48 h | 3  <7 d | 4 <30 d | 5  <1 y | 6 older
-------------+---------+---------+---------+---------+---------+--------
        root |       4 |       0 |       0 |       0 |       0 |       0
Select user name from table or press enter to exit:
root@bt:~#
```

Na obnovu dát zo žurnálovacích systémov ext3 a ext4 je k dispozícii nástroj *extundelete*. Ako už bolo spomenuté, pri forenznej analýze málokedy vieme presnú cestu k súboru, alebo číslo jeho i-uzlu. Preto je pri vyšetrovaní najviac využívaný parameter zaisťujúci obnovu všetkých zmazaných súborov, ktoré sú neskôr analyzované.

```
root@bt:~# extundelete ~/snap/xubuntu.img --restore-all
WARNING: Extended attributes are not restored.
WARNING: EXT3_FEATURE_INCOMPAT_RECOVER is set.
The partition should be unmounted to undelete any files without further
data loss.
If the partition is not currently mounted, this message indicates
it was improperly unmounted, and you should run fsck before continuing.
If you decide to continue, extundelete may overwrite some of the deleted
files and make recovering those files impossible.  You should unmount the
file system and check it with fsck before using extundelete.
Would you like to continue? (y/n)
y
Loading filesystem metadata ... 38 groups loaded.
Loading journal descriptors ... 29966 descriptors loaded.
Searching for recoverable inodes in directory / ...
994 recoverable inodes found.
Looking through the directory structure for deleted files ...
Restored inode 221078 to file RECOVERED_FILES/etc/resolv.conf.v1
Unable to restore inode 221102 (etc/X11/Xresources/x11-common.dpkg-new):
Space has been reallocated.
root@bt:~#
```

Obnovené súbory sú uložené v aktuálnom adresári v *RECOVERED_FILES*, pričom je zachovaná celá cesta k súboru z pôvodného systému.

5.6 Detekcia malware

Ak sa útočníkovi raz podarí dostať do systému, jeho snahou je nechať si otvorený prístup do budúcna. Nechce však, aby toto preniknutie bolo zaznamenané legitímnym správcom napadnutého systému. Preto sa snaží svoju činnosť zamaskovať. Jednou z možností je infekcia systému programami spadajúcimi do kategórie rootkitov. Veľmi rozšírenými sú hlavne LKM rootkity[17]. Medzi najznámejšie patria Adore, Knark a Itf. Rootkity poskytujú útočníkovi rozšírené možnosti, ako napríklad prístup s právami užívateľa root, skrývanie súborov a procesov vo výstupoch programov a veľa iných. V distribúcií BackTrack existujú dva nástroje na detekciu podobných infekcií.

[17] Loadable kernel module je modul rozširujúci možnosti jadra operačného systému. Môže byť dynamicky zavedený do systému používateľom s administrátorskými právami a beží na úrovni jadra.

Prvým nástrojom je program *rkhunter*. Na svoju činnosť využíva databázu hashov súborov, pred prvým spustením je vhodné ju aktualizovať.

```
root@bt:~# rkhunter --update
[ Rootkit Hunter version 1.3.8 ]

Checking rkhunter data files...
  Checking file mirrors.dat                                  [ No update ]
  Checking file programs_bad.dat                             [ Updated ]
  Checking file backdoorports.dat                            [ No update ]
  Checking file suspscan.dat                                 [ No update ]
  Checking file i18n/cn                                      [ No update ]
  Checking file i18n/de                                      [ No update ]
  Checking file i18n/en                                      [ No update ]
  Checking file i18n/zh                                      [ No update ]
  Checking file i18n/zh.utf8                                 [ No update ]
root@bt:~#
```

Program sa pri nepozmenenom chovaní snaží o analýzu bezpečnosti a detekciu malware v systéme v ktorom je spustený. Rovnako vykonáva veľa nepotrebných testov pre forenznú analýzu. Vhodnou zmenou argumentov je možné zmeniť koreňový adresár a skenovať pripojenú forenznú kópiu disku s obmedzeným počtom testov. Program je schopný detekcie viacej ako 70 známych rootkitov. Ich zoznam, rovnako ako popis všetkých testov je možné nájsť v manuálových stránkach programu.

```
root@bt:~# rkhunter -c --enable rootkits -r /media/disk/
[ Rootkit Hunter version 1.3.8 ]
Checking for rootkits...
  Performing check of known rootkit files and directories
   55808 Trojan - Variant A                                  [ Not found ]
   ADM Worm                                                  [ Not found ]
   AjaKit Rootkit                                            [ Not found ]
   Adore Rootkit                                             [ Not found ]

<<výčet kontrolovaných rootkitov je vynechaný >>

   zaRwT.KiT Rootkit                                         [ Not found ]
   ZK Rootkit                                                [ Not found ]

  Performing additional rootkit checks
   Suckit Rookit additional checks                           [ OK ]
   Checking for possible rootkit files and directories       [ None found ]
   Checking for possible rootkit strings                     [ None found ]

  Performing malware checks
   Checking running processes for suspicious files           [ None found ]
   Checking for login backdoors                              [ None found ]
   Checking for suspicious directories                       [ None found ]
   Checking for sniffer log files                            [ None found ]

  Performing Linux specific checks
   Checking loaded kernel modules                            [ Warning ]
   Checking kernel module names                              [ OK ]

<<výstup pokračuje na ďalšej strane>>
```

```
System checks summary
=====================

File properties checks...
    All checks skipped

Rootkit checks...
    Rootkits checked : 238
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 1 minute and 58 seconds

All results have been written to the log file (/var/log/rkhunter.log)

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

root@bt:~#
```

V tomto prípade nebol nájdený ani jeden rootkit. Celý výsledok kontroly je možné zobraziť otvorením logovacieho súboru. V dôsledku existencie rozličných systémov, konfigurácií a verzií jadra môžu byť zobrazené falošné varovania. Rovnako ako všetky bezpečnostné nástroje radšej zobrazuje falošné varovanie ako keby skryl reálnu hrozbu.

Program *chkrootkit* je svojou funkciou podobný. Vykonáva nad systémom sadu testov a zobrazí ich výsledky. Zoznam všetkých možných testov je viditeľný po spustení súboru s vhodným parametrom.

```
root@bt:~# cd /pentest/forensics/chkrootkit
root@bt:/pentest/forensics/chkrootkit# ./chkrootkit -l
./chkrootkit: tests: aliens asp bindshell lkm rexedcs sniffer w55808 wted
scalper slapper z2 chkutmp OSX RSPLUG amd basename biff chfn chsh cron
crontab date du dirname echo egrep env find fingerd gpm grep hdparm su
ifconfig inetd inetdconf identd init killall  ldsopreload login ls lsof
mail mingetty netstat named passwd pidof pop2 pop3 ps pstree rpcinfo
rlogind rshd slogin sendmail sshd syslogd tar tcpd tcpdump top telnetd
timed traceroute vdir w write
root@bt:/pentest/forensics/chkrootkit#
```

Nástroj sa skladá z viacerých súčastí, každá má špecifickú funkčnosť. Ako je vidieť z názvov testov, najväčší dôraz je kladený na kontrolu systémových binárnych súborov na modifikáciu rootkitom. Ďalšie testy sú zamerané na testovanie sieťového adaptéra na promiskuitný mód, na zmazané logovacie súbory a známky trójskych koní. V predvolenom chovaní kontroluje systém z ktorého je spustený, preto je nutné vhodným argumentom zmeniť koreňový adresár.

```
root@bt:/pentest/forensics/chkrootkit# ./chkrootkit -r /media/disk
ROOTDIR is `/media/disk/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected

<<výčet kontrolovaných rootkitov je vynechaný >>

Checking `slapper'... not infected
Checking `z2'... chklastlog: nothing deleted
Checking `chkutmp'...  The tty of the following user process(es) were not
found
 in /var/run/utmp !
! RUID          PID TTY    CMD
!  root                1434  tty8     /usr/bin/X  -nolisten  tcp  :0  -auth
/tmp/serverauth.Jizclw0FON
chkutmp: nothing deleted
Checking `OSX_RSPLUG'... not infected
root@bt:/pentest/forensics/chkrootkit#
```

Opäť vidíme že systém nie je infikovaný, keďže očakávaný výstup je „not found“ alebo „not infected“. *Chkrootkit* produkuje menej falošných alarmov a preto je nutné venovať pozornosť každému varovaniu (detekovanému hlásením INFECTED).

5.7 Analýza extrahovaných dát

Analýzou dát rozumieme interpretáciu extrahovaných dát a ich spracovanie do logického a užitočného formátu. Typ vykonanej analýzy sa líši prípad od prípadu, najčastejšie používanými sú časová analýza, analýza skrytých dát a analýza aplikácií a súborov.[9]

Časová analýza súvisí s vytvorením časovej osi ktorá vyjadruje precedenciu udalostí. Časové informácie sú uložené buď v interných štruktúrach súborového systému (MAC times), alebo v logovacích súboroch, kde tieto informácie zapisujú priamo aplikácie. Veľmi dobrá podpora časovej analýzy je obsiahnutá v komplexných forenzných prostrediach, generovanie časovej osi prináša veľkú pridanú hodnotu pri získavaní prehľadu o činnosti systému.

Analýza skrytých dát je veľmi často zamieňaná s obnovou zmazaných súborov. Zásadným rozdielom je však to, že pri analýze skrytých dát sa pokúšame obnoviť tak veľa informácií, ako sa len dá a následne vybrať to podstatné, zatiaľ čo pri obnove zmazaných súborov existuje predstava čo a kde hľadáme. Navyše do tejto kategórie zapadá aj odhalenie informácií steganograficky skrytých a odhalenie neviditeľných diskových oddielov.

Analýza aplikácií a súborov poskytuje celkový náhľad na využitie operačného systému. Detaily analýzy sú aplikačne špecifické, navyše sa líšia aj v rámci jednej aplikácie v rôznych verziách. Príkladom je vyšetrovanie navštívených webových stránok, kedy sú tieto informácie

ukladané do inej lokácie v prehliadači Firefox aktuálnej verzie (12.0) a predchádzajúcich, stále používaných verzií (4.0).

5.7.1 Extrakcia súborov špecifického typu

Na použitie najjednoduchším nástrojom na extrakciu dát istého typu je nástroj *foremost*. Pri známych súboroch obsahuje definície štruktúry, takže stačí ako parameter zadať typy súborov ktoré požadujeme.

```
root@bt:~# foremost -t jpg,pdf -o ~/output -i ~/snap/xubuntu.img
Processing: /root/snap/xubuntu.img
|*****************************************|
root@bt:~#
```

Výsledkom je výstupný adresár, ktorý obsahuje ďalšie adresáre s vyhľadanými súbormi, roztriedenými podľa typu súboru.

```
root@bt:~# cd output/
root@bt:~/output# ls
audit.txt  jpg  pdf
root@bt:~/output#
```

V súbore audit.txt sú zaznamenané všetky detaily o behu programu, spolu so zhrnutím výsledkov. V jednotlivých adresároch sú už samostatné súbory ktoré program extrahoval a môže na nich pokračovať analýza.

Ostatné nástroje tejto kategórie (scalpel a magicrescue) sú funkcionalitou veľmi podobné, preto im nie je venovaná ďalšia pozornosť.

5.7.2 Steganografia a jej detekcia

V kapitole zaoberajúcej sa bezpečnostnými rizikami je spomenutá snaha skryť obsah súborov použitím šifrovania. Existujú však aj iné metódy, medzi jednu z nich patri steganografia. Ukryť informácie jedného súboru do druhého dokáže viacero steganografických programov. Každý používa iný algoritmus a podporuje rozličné formáty súborov. Detekcia steganografie však už nie je triviálna a na detekciu existuje malé množstvo nástrojov. Príkladom je program *stegdetect*, ktorý toto dokáže.

```
root@bt:~/pics# ls
carrier.jpg  kvetinka.jpg  obr.jpg  sunflowers.jpg  teddybear.jpg
root@bt:~/pics# stegdetect *.jpg
carrier.jpg : negative
kvetinka.jpg : negative
obr.jpg : negative
sunflowers.jpg : f5(***)
teddybear.jpg : negative
root@bt:~/pics#
```

Práve súbor sunflowers.jpg bol využitý na ukrytie iného súboru. *Stegdetect* správne rozpoznal použitie steganografie a súčasne rozpoznal aj nástroj *F5*[18], ktorým bol súbor vytvorený. Obnova tajnej informácie zo súboru nie je úplne triviálna a nie je ani predmetom tejto práce. Je však ukázaná v demonštračnom postupe v prílohe.

[18] vyvinutý na Hochschule für Technik und Wirtschaft v Drážďanoch, dostupný na http://code.google.com/p/f5-steganography/

5.8 Analýza systémových súborov

Linuxové operačné systémy obsahujú množstvo konfiguračných a logovacích súborov, ktoré poskytujú cenné informácie počas forenznej analýzy. Tieto súbory nie sú využívané len samotným operačným systémom, ale aj aplikáciami ako je napríklad webový server *Apache*[19] a rôzne implementácie e-mailového alebo FTP servera. Umiestnenie nižšie spomenutých súborov sa môže líšiť v závislosti na distribúcií operačného systému Linux, keďže každá dodržiava iné konvencie. Ak nie je uvedené inak, predpokladáme distribúciu založenú na Ubuntu 11.10.

5.8.1 Systémové logy

- **System log –** syslog, ktorý zachytáva správy a udalosti zo systému. Zväčša obsahuje najviac informácií spomedzi všetkých logovacích súborov. Umiestnenie*: /var/log/syslog*
- **Messages log –** obsahuje informačné správy od aplikácií a systémových zariadení. Umiestnenie: */var/log/messages*
- **Kernel log –** poskytuje prístup k detailným správam od jadra operačného systému. Informácie z tohto súboru sú nenahraditeľné pri vyšetrovaní napadnutia LKM rootkitom. Umiestnenie: */var/log/kernel.log*
- **Debug log –** obsahuje správy, ktoré umožňujú nízkoúrovňovú kontrolu činnosti systému a aplikácií. Správy v ňom obsiahnuté sú klasifikované ako menej závažné než správy v message logu. Umiestnenie: */var/log/debug*
- **Daemon log –** sú v ňom uložené správy prijaté z daemon aplikácií[20]. Umiestnenie: */var/log/daemon.log*
- **Authentication log –** zaznamenáva činnosť mechanizmov pre autentizáciu používateľov (zvyčajne PAM[21]). Poskytuje cenné informácie o tom, ktorý užívateľ sa kedy na daný systém prihlásil. Umiestnenie: */var/log/auth.log* [11]

5.8.2 Aplikačné logy

Nie je možné zovšeobecniť miesto, kam sa ukladajú záznamy produkované aplikáciami. Pri forenznom vyšetrovaní jednotlivých aplikácií je nutné vyhľadať túto informáciu v dokumentácií. Vhodným miestom sú manuálové stránky danej aplikácie. Veľa aplikácií vytvára logy v adresári /var/log a pomenúva ich názvom podobným názvu aplikácie.

- **Webový server Apache –** Predvolená inštalácia vytvorí adresár */var/log/apache2* a v ňom súbory do ktorých sú ukladané záznamy podľa svojej povahy.

[19] Najčastejšie používaný webový server na svete podľa http://news.netcraft.com/, dostupný na http://httpd.apache.org/

[20] Daemon aplikácia je program bežiaci na pozadí (bežný užívateľ o jeho existencii často nevie), vykonávajúci operácie potrebné na správnu funkciu systému.

[21] Pluggable Authentication Modules, systém slúžiaci na autentizáciu užívateľov, viac informácií na http://www.kernel.org/pub/linux/libs/pam/whatispam.html

- */var/log/apache2/access.log* – v ktorom sú zaznamenané všetky klientom odoslané správy a súbory načítané webovým serverom. V logoch je zaznamená aj IP adresa klienta, takže je možné identifikovať kam smerovala komunikácia.
- */var/log/apache2/error.log* – do ktorého sú ukladané chyby ktoré sa počas behu servera vyskytli

- **Tlačový systém CUPS**[22] **–** predvolene vytvorí adresár */var/log/cups* v ktorom ukladá detailné informácie o činnosti. Obsiahnuté správy sú častejšie využívané pri odstraňovaní problémov s tlačou, každopádne vyšetrovanie využívania periférnych zariadení ako je tlačiareň je aj predmetom forenznej analýzy.
  - */var/log/cups/access_log* – je podobný access logu webového serveru – rovnako zaznamenáva zdroje ku ktorým bolo pristupované.
  - */var/log/cups/page_log* – v ktorom sú uvedené informácie o všetkých stránkach ktoré boli poslané na tlačiareň participujúcu v tlačovom systéme.
  - */var/log/cups/error_log* – zaznamenáva chyby pri tlači
- **FTP server pure-FTPd**[23] **–** svoju činnosť zaznamenáva (ak nie je konfiguračným súborom dané inak) len do jedného súboru, ktorým je */var/log/pure-ftpd/transfer.log*. V záznamoch je ukladaná IP adresa vzdialeného počítača, meno užívateľa, časový odtlačok, použitá metóda, prenášaný súbor a chybový kód.
- **História príkazového riadku** – užívatelia s interaktívnym prístupom do systému majú priradený príkazový riadok. Existuje viacero implementácií, v každej distribúcií sa zvyčajne nachádza viacej príkazových riadkov ako jeden, pre možnosť voľby. Implementáciu príkazového riadku, ktorý je priradený k užívateľovi je možné zistiť v súbore */etc/passwd* nižšie uvedeným spôsobom.

```
root@bt:/media/disk# cat etc/passwd | grep -E 'root|martin'
root:x:0:0:root:/root:/bin/bash
martin:x:1001:1001::/home/martin:/bin/sh
root@bt:/media/disk#
```

Na výstupe vidíme že používateľ martin má priradený Bourne shell (*/bin/sh*), zatiaľ čo správca systému root používa Bourne-Again shell (*/bin/bash*). Bourne-Again shell históriu príkazov ukladá do súboru *.bash_history* v domovskom adresári. Umiestnenie súborov z históriou príkazov pre iné implementácie je nutné zistiť v dokumentácii.

```
root@bt:/media/disk/root# ls -al | grep bash
-rwx---rwx  1 root root 14450 2012-05-05 19:56 .bash_history
-rwx---rwx  1 root root  3186 2011-05-09 08:51 .bashrc
root@bt:/media/disk/root#
```

5.8.3 SUID a SGID súbory

SUID a SGID sú príznaky prístupových práv, umožňujúce spustenie súboru s právami jeho vlastníka (SUID) alebo s právami skupiny jeho vlastníka (SGID). Umožňujú teda spustenie programov s dočasne zvýšenými právami. Často uvádzaným prípadom kedy je nutná existencia SUID je program

[22] Open source tlačový systém vyvinutý spoločnosťou Apple. Dostupný na http://www.cups.org/

[23] File transfer protocol server dostupný pod licenciou BSD, bežne používaný v prostredí operačného systému Linux, dostupný na http://www.pureftpd.org/project/pure-ftpd

passwd, ktorý zaručí užívateľovi s neprivilegovaným prístupom zmeniť súbor */etc/shadow*, ktorého vlastníkom je užívateľ root.

Príznaky nastavené na nevhodných súboroch sú často krát zdrojom útokov typu privilege-escalation. SUID príznak nastavený na príkazový riadok *(/bin/bash*) umožní každému užívateľovi ktorý ho spustí prístup k systému s právami užívateľa root. Kontrola systému sa vykonáva pomocou programu find, ktorý na výstup dodá všetky súbory s požadovanými právami.

```
root@bt:~# find /media/disk/ -type f -perm -04000 -print
/media/disk/usr/bin/pkexec
/media/disk/usr/bin/passwd
/media/disk/usr/bin/sudoedit
/media/disk/usr/bin/arping
/media/disk/usr/bin/chsh
/media/disk/usr/bin/sudo
/media/disk/usr/bin/X
/media/disk/usr/bin/traceroute6.iputils
/media/disk/usr/bin/newgrp
/media/disk/usr/bin/gpasswd
/media/disk/usr/bin/at
/media/disk/usr/bin/lppasswd
/media/disk/usr/bin/chfn
/media/disk/usr/bin/mtr
/media/disk/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/media/disk/usr/lib/pt_chown
/media/disk/usr/lib/eject/dmcrypt-get-device
/media/disk/usr/lib/policykit-1/polkit-agent-helper-1
/media/disk/usr/lib/openssh/ssh-keysign
/media/disk/usr/sbin/uuidd
/media/disk/usr/sbin/pppd
/media/disk/bin/su
/media/disk/bin/umount
/media/disk/bin/mount
/media/disk/bin/ping6
/media/disk/bin/fusermount
/media/disk/bin/ping
root@bt:~# find /media/disk/ -type f -perm -06000 -print
/media/disk/usr/bin/X
/media/disk/usr/bin/at
/media/disk/usr/sbin/uuidd
root@bt:~#
```

U niektorých programov je nutnosť nastavenia SUID zrejmá. U iných ako napríklad *ping* a *traceroute* (a ich verzie pre IPv6[24]) nie je až tak viditeľná, ale potrebná pre úspešné otvorenie soketu schopného práce s ICMP[25] správami.

[24] Internet protocol, version 6, protokol tretej vrstvy modelu ISO/OSI špecifikácia dostupná na: http://www.ietf.org/rfc/rfc2460.txt

[25] Internet control message protocol, protokol tretej vrstvy modelu ISO/OSI špecifikácia dostupná na: http://www.ietf.org/rfc/rfc792.txt

5.9 Vypracovanie forenzného posudku

Zhrnutím celého úsilia je vytvorenie štúdie, ktorá obsahuje všetky relevantné informácie prípadu a nazýva sa forenzný posudok. Cieľom je oboznámiť čitateľa o postupe a výsledkoch. Okrem faktov je žiaduce, ale nie nevyhnutné aby posudok obsahoval aj názory experta na výsledky štúdie. Ak sú dostupné svedecké výpovede, veľmi často nie sú uvedené priamo v posudku, ale je na ne len odkazované.

Ako pri každej písanej správe musí byť autorovi jasné pre koho a za akým účelom je správa tvorená. Celý obsah správy tomuto musí byť prispôsobený. Ak bude čitateľ osoba s neveľkým technickým vzdelaním, niektoré kapitoly musia byť venované vysvetleniu problematiky.

Forenzné posudky by vždy mali začínať formuláciou požiadaviek zadávateľa a stanovením cieľov. Jasne stanovené ciele znižujú celkove vyvinuté úsilie a celkové náklady vynaložené na vyšetrovanie.

Štruktúra dokumentu nie je pevne daná. Líši sa v závislosti na cieľovej skupine, vyšetrovanom prípade a rozsahu posudku. Základnou štruktúrou prevzatou z literatúry [3] je:

- Abstrakt
- Obsah
- Telo dokumentu
- Záver
- Referencie
- Slovník pojmov
- Poďakovania
- Prílohy

Niektoré body bývajú veľmi často vynechané, napríklad pri posudkoch, ktoré nepresahujú niekoľko strán sa vynecháva abstrakt a obsah.

Telo dokumentu obsahuje zasvätenie čitateľa do problematiky a jeho oboznámenie s prípadom. Je v ňom predstavený problém a popísaný spôsob riešenia smerom od všeobecných k špecifickým krokom. Kroky na seba logicky nadväzujú a prechod od jedného k druhému je vysvetlený. Myšlienky sú zoskupované do väčších celkov, členených do blokov a sekcií. Pri písaní nie je vhodné používať vágne vyjadrenia alebo priveľmi veľké zovšeobecnenia, autor musí zaujať objektívny postoj k riešenému problému.

Na záver treba dodať, že forenzný posudok je písomný dokument ako každý iný. Mal by spĺňať základné požiadavky na prehľadnú štruktúru typograficky korektné formátovanie textu.

6 Záver

V tejto práci boli rozobrané základné princípy a postupy forenznej analýzy. Vidíme, že pri včasnej identifikácií bezpečnostných rizík a vyvarovaní sa chýb je možné zo operačného systému Linux získať veľké množstvo informácií použiteľných v právnom procese.

Získavanie týchto informácií nie je podmienené vysokými investíciami do hardwarového alebo softwarového vybavenia. Existujú voľne dostupné nástroje, ktorých vlastnosti sú porovnateľné s komerčnými nástrojmi. Veľké množstvo nástrojov je zahrnutých v distribúcii BackTrack, na ktorej bolo použitie aplikácií demonštrované.

Vyšetrovanie pomocou nástrojov v distribúcii BackTrack nie je obmedzené len na vyšetrovanie systémov založených na Linuxe. Rovnako dobre sa dajú použiť na vyšetrovanie iných systémov, nevynímajúc ani vstavané a mobilné zariadenia. Spomínaná oblasť je stále viac potrebná, keďže počet týchto zariadení rýchlo vzrastá.

Výsledok všetkého úsilia je zhrnutý vo forenznom posudku. Veľmi často je prínos vykonanej analýzy hodnotený práve podľa konečného posudku. V práci je okrajovo popísaná metodika tvorby štúdie a príklad posudku je priložený. Druhou prílohou sú demonštračné úlohy ktoré môžu byť použité pri vyučovaní.

Budúcnosť forenzného vyšetrovania vidím v prechode od analýzy vypnutého systému k live analýze. Zmena metódy je podmienená stále sa zvyšujúcou mierou ochrany informácií pred zneužitím (šifrovanie súborov a celých diskových jednotiek). Z uvedeného vyplývajú nielen zvýšené nároky na znalosti a schopnosti vyšetrovateľov, ale aj potreba odlišných nástrojov.

Literatúra

[1] PROSISE, Chris, Kevin MANDIA a Matt PEPE. *Incident Response*. 2nd ed. New York ;: London, c2003, 507 s. ISBN 00-722-2696-X.

[2] BROWN, Christopher L. *Computer evidence*: *collection and preservation*. 2nd ed. Boston: Charles River Media, c2010, 518 s. ISBN 978-158-4506-997.

[3] PHILLIPS, Amelia, Bill NELSON a Frank ENFINGER. *Guide to computer forensics and investigations*. 2nd ed. Boston (Mass.): Thomson Course Technology, 2006. ISBN 978-061-9217-068.

[4] PATE, Steve D. *Unix filesystems*: *evolution, design, and implementation (VERITAS series)*. Indianapolis: J. Wiley, c2003, 443 s. ISBN 04-711-6483-6.

[5] GNU core utilities. *The GNU Operating System* [online]. 13.1.2011 [cit. 2012-03-19]. Dostupné z: http://www.gnu.org/software/coreutils/coreutils.html

[6] The Field Guide for Investigating Computer Crime: Search and Seizure Planning (Part 4). WRIGHT, Timothy. SYMANTEC. *Symantec Connect Community* [online]. [cit. 2012-04-11]. Dostupné z: http://www.symantec.com/connect/articles/field-guide-part-four

[7] SWGDE. *Scientific Working Group on Digital Evidence* [online]. [cit. 2012-04-11]. Dostupné z: http://www.swgde.org/documents/current-documents/

[8] Presentations Archive. *Simson Garfinkel's web site* [online]. [cit. 2012-04-11]. Dostupné z: http://simson.net

[9] RISK ANALYSIS CONSULTANTS. *Forenzní zkoumání digitálních důkazů*: *Příručka vyšetřovatele* [online]. 30. 12. 2005 [cit. 2012-04-15]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/883AABB42333CB35C12570FC0034A328/$FILE/Guide%20051230.pdf

[10] Loopback Devices in Linux. NGUYEN, Paul. CALIFORNIA STATE UNIVERSITY LONG BEACH. *Paul Nguyen at CSULB* [online]. [cit. 2012-04-19]. Dostupné z: http://csulb.pnguyen.net/loopbackDev.html

[11] Community Ubuntu Documentation: LinuxLogFiles. *Official Ubuntu Documentation* [online]. 2011 [cit. 2012-05-05]. Dostupné z: https://help.ubuntu.com/community/LinuxLogFiles

Zoznam príloh

Zoznam obrázkov

Príloha č.1

POSUDOK FORENZNEJ ANALÝZY PRE SPOLOČNOSŤ ACME S.R.O.

Vyšetrovateľ: Martin Beneš

Dátum: 12. máj 2012

Obsah

1 Incident

1.1 Popis prípadu

Spoločnosť ACME s.r.o. sa zaoberá návrhom, výrobou a predajom elektronických súčiastok. Keďže ide o odbor ktorý vyžaduje neustále inovácie, aby spoločnosť udržala krok s konkurenciou vzniklo vlastné vývojové oddelenie. Toto oddelenie sa zaoberá návrhom a registrovaním nových patentov a priemyslových vzorov. Pri registrácií posledných patentov sa však zistilo, že v nedávnej minulosti veľmi podobné patenty už boli registrované najväčšou konkurenčnou firmou. Vzniklo preto podozrenie z úniku dôverných informácií. Externým auditom bolo potvrdené, že sieťové a serverové systémy spoločnosti neboli napadnuté útočníkom a rovnako ani nebol zaznamenaný pokus a takéto preniknutie. Po zvážení ostatných možností sa jediným možným spôsobom, ako sa informácie dostali mimo spoločnosti stalo ich úmyselné vynesenie niektorým zamestnancom. Interným vyšetrovaním sa okruh podozrivých osôb zmenšil na jednu osobu. Hlavným podozrivým sa stal Miroslav Starý, ktorého počítač bol identifikovaný ako miesto, odkiaľ s najväčšou pravdepodobnosťou informácie unikli.

Úlohou forenzného vyšetrovania je na základe digitálnych informácií prítomných v počítači potvrdiť alebo vyvrátiť toto podozrenie. V obidvoch prípadoch je nutné vytvoriť správu a uchovať dôkazy pre možný súdny proces.

1.2 Dôkazný materiál

Spoločnosť ACME s.r.o. ako hlavný dôkazný materiál poskytla počítač svojho zamestnanca Miroslava Starého vo vypnutom stave. Týmto je znemožnená live analýza systému a bola vyrobená forenzná kópia disku, podrobená vyšetrovaniu v laboratóriu na forenznej stanici.

1.3 Špecifikácia prípadu

Zadávateľ: ACME s.r.o.
Systém: notebook Fujitsu Amilo Si BS032, sériové číslo YSOL051441
Pripojené periférne zariadenia:
bezdrôtové polohovacie zariadenie Logitech
interná DVD mechanika
čítačka kariet SD a MMC
Dostupné rozhrania:
1x IEEE 1394
1x DVI
1x RJ-11
1x RJ-45
4x USB 2.0
1x PCMCIA
Operačný systém: Xubuntu 11.10
Architektúra: i386 (32-bit)
Súborový systém: ext3
Veľkosť systému: 4,1 GB
Md5 hash: 28d03672a58f1788d1ebfbccf2db6884
Sha1 hash: 8b1e5e6aa79650f1aac33788a35e3a770194ec8f
Podozrenie: únik interných dokumentov v obrazovom formáte

Vyšetrovateľ: Martin Beneš
Miesto prvotného zaistenia dôkazov: pracovné miesto zamestnanca v centrále zadávateľa
Miesto vyšetrovania: forenzné laboratórium
Použité nástroje:
live DVD distribúcie BackTrack 5 R2 spustené v móde blokujúcom zápis na disk
forenzná stanica s nainštalovanou distribúciou BackTrack 5R2

Prípad prijatý: 11. máj 2012
Prípad otvorený: 12. máj 2012
Prípad ukončený: 12. máj 2012

2 Priebeh vyšetrovania

Dňa 10. mája 2012 bola firmou ACME s.r.o. zadaná požiadavka na vyšetrenie úniku firemných dát. Interným vyšetrovaním bol určený hlavný podozrivý – Miroslav Starý, zamestnanec firmy. Cieľom vyšetrovania je získať dôkazy potvrdzujúce podozrenie.

Prvotná obhliadka pracovného miesta bola vykonaná mimo pracovnej doby zamestnanca, aby bolo vylúčené zasiahnutie do prípadu. Počas nej bolo zistené, že okrem polohovacieho zariadenia nie sú k počítaču pripojené žiadne iné periférne zariadenia. Počítač je vo vypnutom stave, pripojený k zdroju elektrickej energie.

2.1 Live analýza

Vzhľadom k tomu že systém bol nájdený vo vypnutom stave, analýza zapnutého systému nie je možná. Všetky informácie sú získané zo snímky disku.

2.2 Získanie dát

Zber dát vyšetrovateľ vykonal použitím Live DVD distribúcie BackTrack. Zapnutím počítača bol sprístupnený BIOS, v ktorom bola pozmenená sekvencia prehľadávaných zariadení a bootovanie z optickej mechaniky nastavené ako preferované. Do jedného z dostupných USB rozhraní bola pripojená pamäť, ktorej súborový systém bol následne pripojený k súborovému systému distribúcie. Duplikácia dát bola vykonaná programom *dd*, pričom zdrojovým oddielom bol oddiel */dev/sda1* a výsledný súbor bol uložený na pripojený USB kľúč. Kópia je verifikovaná porovnaním md5 a sha1 hashu diskového oddielu a forenznej kópie. Kontrolná verifikácia bola vykonaná rovnako po prenesení snímky disku do systému, na ktorom prebieha forenzné vyšetrovanie (forenzná stanica). Bitová kópia je priložená na DVD, v súbore *evidence/image/xubuntu.img*.

2.3 Forenzné vyšetrovanie

Spoločnosť ACME s.r.o. vytvára elektronické schémy špecializovanými nástrojmi určenými na návrh obvodov. Tento nástroj je však dostupný len obmedzenému počtu zamestnancov. Väčšina zamestnancov spoločnosti prichádza do styku s dokumentmi exportovanými do bežných grafických formátov.

Na vyšetrovanie boli použité voľne dostupné nástroje, ktoré sú obsiahnuté v distribúcii operačného systému BackTrack 5 R2.

Pri získavaní kópie disku počítača bol vyšetrovateľ oboznámený s pokročilými znalosťami operačného systému Linux podozrivej osoby. Tento fakt podnietil kontrolu systému na infekciu rootkitmi. Výsledky boli negatívne, žiaden známy rootkit nebol v systéme objavený (pomocou programov chkrootkit a rkhunter). Výsledky kontroly sú dostupné v súboroch *rkhunter_check.txt* a *chkrootkit_check.txt*.

Forenzná kópia disku bola podrobená ďalším testom. Ako prvý bol na získanie informácií použitý nástroj bulk_extractor. V histogramoch, ktoré sú výstupom tohto programu, neboli zistené žiadne nezvyčajne vysoké počty použitia e-mailových adries alebo doménových mien.

Pre účely ďalšieho vyšetrovania bola forenzná kópia pripojená (v režime umožňujúcom len čítanie) k súborovému systému forenznej stanice na ktorej prebehli ďalšie testy. Zoznam všetkých existujúcich súborov sa nachádza v súbore *files.lst*.

Bližšia špecifikácia systému, určená skúmaním štruktúry disku a obsahom súborov */var/log/dmesg* a */etc/lsb-release*, je distribúcia Xubuntu 11.10 (Ubuntu s pracovným prostredím Xfce). Verzia jadra je 3.0.0-12.20-generic.

Keďže informácie unikli v grafickej podobe v súboroch typu jpg, pomocou programov na extrakciu dát boli z diskového oddielu vybrané (pomocou nástroja *scalpel*) všetky súbory, štruktúrou odpovedajúce obrázkom jpg. Po následnom preskúmaní obrazového materiálu vyšetrovateľom ani jeden zo súborov nebol klasifikovaný ako podozrivý.

- **Počet nájdených súborov odpovedajúcich definícii:** 754
- **Veľkosť adresára so súbormi:** 109,1 MB
- **Charakteristika:** obrázky využívané operačným systémom alebo aplikáciami, tlačidlá grafických užívateľských rozhraní, fotografie prírody

Vyšetrovanie pokračovalo analýzou logovacích súborov operačného systému. Pozornosť bola venovaná hlavne sieťovým aplikáciám, keďže predmetom vyšetrovania je únik dát. V systéme nebola zaznamenaná prítomnosť webového servera. Rovnako nebol spustený ssh deamon, umožňujúci prenos súborov bezpečnou cestou založenou na ssh tuneli. Zaznamenaná však bola prítomnosť FTP servera (implementácie pure-FTPd[1]). Analýza logovacieho súboru ukázala prenos súborov medzi počítačom a vzdialeným systémom.

```
root@bt:/media/disk/var/log/pure-ftpd# cat transfer.log
ip4-83-240-113-169.cust.nbox.cz  -  anonymous  [08/May/2012:21:59:31  +0200]
"GET /home/ftpusers/anonymous/DSC03178.jpg" 200 1239424
ip4-83-240-113-169.cust.nbox.cz  -  anonymous  [08/May/2012:21:59:31  +0200]
"GET /home/ftpusers/anonymous/DSC03205.jpg" 200 1113373
ip4-83-240-113-169.cust.nbox.cz  -  anonymous  [08/May/2012:21:59:34  +0200]
"GET /home/ftpusers/anonymous/DSC03248.jpg" 200 504332
ip4-83-240-113-169.cust.nbox.cz  -  anonymous  [08/May/2012:21:59:41  +0200]
"GET /home/ftpusers/anonymous/DSC03503.jpg" 200 985538
ip4-83-240-113-169.cust.nbox.cz  -  anonymous  [08/May/2012:22:06:43  +0200]
"PUT /home/ftpusers/anonymous/file.zip" 200 142
root@bt:/media/disk/var/log/pure-ftpd#
```

Z výpisu je viditeľné, že FTP server zaslal klientovi štyri súbory s príponou jpg a prijal súbor s príponou zip. Prenos sa odohral 8. mája 2012 medzi 21:59 a 22:06. Dátum a čas zapadá do intervalu časovej osi poskytnutej zadávateľom, v ktorom sa mohol únik odohrať. Na autentizáciu bolo použité meno a heslo *anonymous*, čo je štandardom pre anonymné dátové prenosy. Bližšie určenie počítača do ktorého boli súbory prenesené nie je možné zistiť. Jediný záchytný bod je doménové meno počítača, pre ktoré vyšetrovateľ overil IP adresu. Dotaz na DNS server vrátil IP adresu obsiahnutú v DNS zázname.

[1] http://www.pureftpd.org/project/pure-ftpd

```
root@bt:/media/disk/var/log/pure-ftpd#       nslookup       ip4-83-240-113-
169.cust.nbox.cz
Server:         8.8.4.4
Address:        8.8.4.4#53

Non-authoritative answer:
Name:   ip4-83-240-113-169.cust.nbox.cz
Address: 83.240.113.169

root@bt:/media/disk/var/log/pure-ftpd#
```

Pri pokuse o získanie súborov vyšetrovateľ zistil, že súbory boli odstránené. Po zmene adresára podľa informácie v logu bol nájdený len prázdny adresár.

```
root@bt:/media/disk/home/ftpusers/anonymous# ls -al
total 8
drwxrwxrwx 2 root   root   4096 2012-05-08 22:07 .
drwxr-xr-x 3 martin martin 4096 2012-05-08 20:29 ..
root@bt:/media/disk/home/ftpusers/anonymous#
```

Počas prvotnej časti vyšetrovania vyšlo najavo, že na diskovom oddiele je použitý súborový systém ext3. Programom extundelete bol vykonaný pokus o obnovu všetkých odstránených súborov. Všetkých päť súborov prítomných v logu sa podarilo obnoviť. Otvorením súborov v prehliadači fotografií sa ukázalo že ide o fotografie prírody. Obnovené súbory sú v adresári *evidence/recovered* a ukážka v obrazovej prílohe posudku.

```
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# ls -al
total 3788
drwxr-xr-x 2 root root    4096 2012-05-12 00:03 .
drwxr-xr-x 3 root root    4096 2012-05-12 00:03 ..
-rw-r--r-- 1 root root 1239424 2012-05-12 00:03 DSC03178.jpg
-rw-r--r-- 1 root root 1113373 2012-05-12 00:03 DSC03205.jpg
-rw-r--r-- 1 root root  504332 2012-05-12 00:03 DSC03248.jpg
-rw-r--r-- 1 root root  985538 2012-05-12 00:03 DSC03503.jpg
-rw-r--r-- 1 root root     142 2012-05-12 00:03 file.zip
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous#
```

Keďže jedinými odoslanými súbormi sú vyššie uvedené súbory, vyšetrovateľ na ne zameral svoju pozornosť. Otvorením v nástroji hexedit neboli nájdené podozrivé vzory v štruktúre súborov. Tento záver sa však už nedá vysloviť pre testovanie súborov programom stegdetect. Program detekoval vstavanie inej informácie do súboru metódou vlastnou programu *F5*[2].

```
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# stegdetect *.jpg
DSC03178.jpg : f5(***)
DSC03205.jpg : f5(***)
DSC03248.jpg : f5(***)
DSC03503.jpg : f5(***)
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous#
```

Nástroj *F5* je voľne dostupný pod licenciou GNU Lesser GPL. Jeho použitím bola vyšetrovateľom vykonaná extrakcia dát z pôvodného súboru. Program F5 z každého súboru vytvoril reverzným algoritmom ďalší súbor. Následnou analýzou vzniknutého súboru v programe hexedit hlavička ukázala, že ide znova o grafické súbory typu jpg. Po zobrazení v prehliadači obrázkov bolo zistené, že súbory obsahujú zakreslené elektrické obvody. Tieto vstavané súbory sa nachádzajú v adresári *evidence/embedded* a tiež v obrazovej prílohe.

Súbory s podobným názvom boli zaznamenané v domovskom adresári používateľa *miro*. Skúmanie prístupových práv ukázalo, že do tohto adresára má právo zápisu len vlastník s ID 1000,

[2] Dostupný na http://code.google.com/p/f5-steganography/

ktorým je v afektovanom systéme práve používateľ *miro*. Vo výpisoch programov sú uvedené iné používateľské mená, konkrétne tie, ktoré odpovedajú identifikátorom užívateľov na forenznej stanici. Pri mapovaní UID na meno používateľa je nevyhnutné použiť súbor */etc/passwd* na vyšetrovanom systéme.

```
root@bt:/media/disk/home# ls -al
total 16
drwxr-xr-x  4 root     root     4096 2012-05-08 20:28 .
drwxr-xr-x 23 root     root     4096 2012-05-08 19:53 ..
drwxr-xr-x  3 martin   martin   4096 2012-05-08 20:29 ftpusers
drwxr-xr-x 20 postgres postgres 4096 2012-05-08 21:52 miro
root@bt:/media/disk/home# stat miro
  File: `miro'
  Size: 4096            Blocks: 8          IO Block: 4096   directory
Device: 700h/1792d      Inode: 253405      Links: 20
Access: (0755/drwxr-xr-x)  Uid: ( 1000/postgres)   Gid: ( 1000/postgres)
Access: 2012-05-08 21:52:02.000000000 +0200
Modify: 2012-05-08 21:52:00.000000000 +0200
Change: 2012-05-08 21:52:00.000000000 +0200
root@bt:/media/disk/home# cd ..
root@bt:/media/disk# cat etc/passwd | grep 1000
miro:x:1000:1000:Miroslav Stary,,,:/home/miro:/bin/bash
root@bt:/media/disk#
```

Programom *stegdetect* vyšetrovateľ preveril súbory názvom podobné súborom obnoveným z disku. Vyšlo najavo, že identické (overené md5 hashom) súbory sa nachádzajú v podadresári *Pictures* domovského adresára, do ktorého má právo zápisu len jeho majiteľ.

Z posledného záznamu v logovacom súbore FTP servera je zrejmé, že dáta neboli len sťahované, ale jeden súbor s názvom *file.zip* bol aj nahraný. Tento súbor bol taktiež zmazaný. Keďže počas obnovy zmazaných dát neboli špecifikované jednotlivé súbory, tak aj tento archív bol obnovený. Na rozbalenie bol použitý štandardný nástroj *unzip*. Archív obsahuje jediný súbor s názvom *file.txt*, ktorý je textovým súborom a obsahuje text potvrdzujúci príjem materiálov.

```
root@bt:~# cd RECOVERED_FILES/home/ftpusers/anonymous/
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# ls
DSC03178.jpg  DSC03205.jpg  DSC03248.jpg  DSC03503.jpg  file.zip
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# unzip file.zip
Archive:  file.zip
 extracting: file.txt
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# cat file.txt
Material prisiel vporiadku.
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous#
```

Elektrické obvody extrahované z fotografií boli identifikované zamestnávateľom ako dôverný materiál ktorý unikol.

3 Záver

Cieľom forenzného vyšetrovania bolo určiť, či bol únik interných informácií realizovaný z počítača podozrivého zamestnanca a ak áno poskytnúť dôkazy.

Analýzou systému vyšetrovateľ zistil, že počítač používa operačný systém Linux, distribúciu Xubuntu 11.10. V systéme je nainštalovaný FTP server (pure-FTPd). Kontrolou jeho logovacieho súboru bol zistený uskutočnený prenos dát štyroch grafických súborov zo systému k vzdialenému počítaču a prenos jedného archívu opačným smerom. Prenos súborov z počítača sa odohral 8. mája 2012 o 21:59. Steganografická analýza detekovala vloženie dát do grafických súborov algoritmom vlastným nástroju F5. Reverzné spustenie programu F5 bolo úspešné, výstupom sú štyri súbory obsahujúce grafické zobrazenie elektrických obvodov vo formáte jpg. Identické súbory boli nájdené v adresári do ktorého má právo zápisu len podozrivá osoba, čo vylučuje možnosť vloženia iným používateľom.

Extrahované elektrické obvody boli predložené zadávateľovi, ktorý potvrdil, že ide o materiál ktorý obsahom odpovedá materiálu uniknutému zo spoločnosti ku konkurencii. Ďalšie právne kroky sú v zodpovednosti zamestnávateľa.

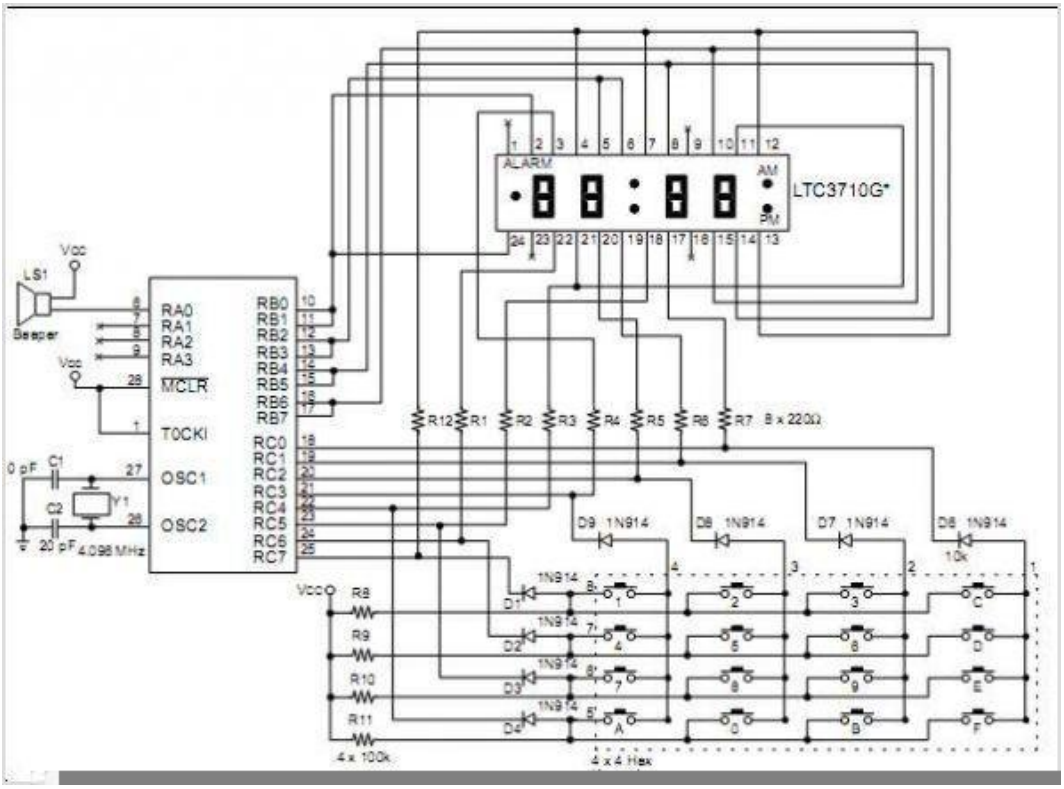
4 Obrazová príloha

Obr. 1: Dôkazný materiál – počítač podozrivej osoby, vrchná strana

Obr. 2: Dôkazný materiál – počítač podozrivej osoby, spodná strana

Obr. 3: Dôkazný materiál – počítač podozrivej osoby, detail sériového čísla a typu

Obr. 4: Súbor DSC03248.jpg: pôvodne zmazaný súbor obsahujúci vstavanú informáciu



Obr. 5: Súbor 03: súbor vytvorený reverzným spustením programu *F5*

Zoznam obrázkov

Príloha č.2

Demonštračné úlohy forenznej analýzy

Tento dokument vznikol ako príloha bakalárskej práce „Forenzní analýza v operačních systémech Linux“. Slúži ako výukový materiál a sú v ňom rozobrané postupy a princípy forenznej analýzy. Predpokladá sa užívateľská znalosť operačného systému Linux, rovnako grafického prostredia ako aj príkazového riadku.

Úlohy sú zamerané na analýzu vypnutého systému s pomocou distribúcie BackTrack. Počas vyučovania je možné použiť voľne dostupné live DVD distribúcie, alebo vykonávať analýzu z forenznej stanice s nainštalovaným operačným systémom. V demonštračných úlohách bude predpokladaná druhá možnosť.

Ak nie je uvedené inak, forenzná kópia je vytvorená z diskového oddielu so súborovým systémom ext3 pomocou nástroja *dd*, md5 a sha1 hashe boli spočítané a porovnané s pôvodným diskovým oddielom. Odkazovaná príloha je v adresári *evidence/image* nachádzajúceho sa na DVD nosiči priloženom k technickej správe bakalárskej práce a bola skopírovaná do adresára */root/image*. Prihlasovacie údaje do inštalácie systému BackTrack sú root/toor.

Metodický úvod

Uvedené úlohy na seba nadväzujú. Aby nedošlo k zanášaniu chýb do nasledujúcich úloh, odporúča sa zbežná kontrola každej dokončenej úlohy cvičiacim počas práce. Informácie o použití jednotlivých programov je možné získať z dokumentácie, keďže ide o nástroje v OS Linux, dokumentácia je obsiahnutá v manuálových stránkach. Nástroje sú dostupné spustením z príkazového riadku, alebo z menu distribúcie.

1. Overenie vzdialeného prístupu do systému

V tejto úlohe je cieľom overiť možnosti vzdialenej komunikácie so systémom (vyšetrovanie obmedzíme na ssh sever, FTP server a webový server).

a. Pripojte forenznú kópiu disku k systému forenznej stanice na loopback zariadenie, do adresára */media/disk*. Zabráňte pozmeneniu kópie pripojením v režime read-only.
b. Prehľadaním súborového systému zistite aký software je inštalovaný.
c. Analyzujte logovací súbor nájdeného softwaru.

Pripojenie forenznej kópie bolo vykonané príkazom_____.
V systéme je nainštalovaný _____ server, konkrétne implementácia _____ .
Logovací súbor je umiestnený v adresári _____ a má názov _____.
Jeho obsahom je:

Riešenie:

Forenznú kópiu pripojíme pomocou nástroja *mount*:

```
mount -t ext3 -o ro,loop,noatime ~/snap/xubuntu.img /media/disk
```

Prehľadaním súborového systému (hlavne adresára */etc/init.d/*) sa dá zistiť, že jediným inštalovaným serverom je FTP server v implementácií pure-FTPd.

Logovanie prebieha do súboru */media/disk/var/log/pure-ftpd/ transfer.log*, ktorého obsahom je:

```
root@bt:/media/disk/var/log/pure-ftpd# cat transfer.log
ip4-83-240-113-169.cust.nbox.cz - anonymous [08/May/2012:21:59:31 +0200] "GET
/home/ftpusers/anonymous/DSC03178.jpg"200 1239424
ip4-83-240-113-169.cust.nbox.cz - anonymous [08/May/2012:21:59:31 +0200] "GET
/home/ftpusers/anonymous/DSC03205.jpg"200 1113373
ip4-83-240-113-169.cust.nbox.cz - anonymous [08/May/2012:21:59:34 +0200] "GET
/home/ftpusers/anonymous/DSC03248.jpg"200 504332
ip4-83-240-113-169.cust.nbox.cz - anonymous [08/May/2012:21:59:41 +0200] "GET
/home/ftpusers/anonymous/DSC03503.jpg"200 985538
ip4-83-240-113-169.cust.nbox.cz - anonymous [08/May/2012:22:06:43 +0200] "PUT
/home/ftpusers/anonymous/file.zip" 200142
root@bt:/media/disk/var/log/pure-ftpd#
```

2. Obnova zmazaných súborov

V operačných systémoch Linux je rušenie súborov zaistené volaním *unlink*. Pri mazaní súboru odstráni pevný odkaz medzi menom súboru a i-uzlom. Systém udržuje informáciu o počte procesov, ktoré používajú daný súbor. Ak počet mien a počet procesov ktoré používajú súbor klesne na nulu, i-uzol a bloky ktoré súbor zaberal sú uvoľnené. Forenzná kópia bola vytvorená z disku so súborovým systémom ext3, zohľadnite túto skutočnosť pri obnove súborov.

a. Zmeňte pracovný adresár na adresár v ktorom sú súbory obsiahnuté v logoch serveru z predchádzajúcej úlohy.
b. Overte prítomnosť súborov programom *ls*.
c. Ak bol niektorý zmazaný, pokúste sa o obnovu programom *extundelete*.
d. Ak obnovenie prebehlo v poriadku, zobrazte súbory v prehliadači obrázkov.

Zmena pracovného adresára sa vykoná príkazom _____.
Adresár obsahuje _____súborov.
Zmazané súbory je možné obnoviť príkazom _____.

Riešenie:

Do adresára odkiaľ boli stiahnuté súbory sa dostaneme pomocou *cd*, v adresári sa nachádza 0 súborov.

```
root@bt:~# cd /media/disk/home/ftpusers/anonymous/
root@bt:/media/disk/home/ftpusers/anonymous# ls -a
.  ..
root@bt:/media/disk/home/ftpusers/anonymous#
```

Obnova všetkých zmazaných súborov nástrojom *extundelete* vyzerá ako je uvedené nižšie. Je však možné obnoviť súbory jednotlivo, zadaním ich cesty.

```
root@bt:/media/disk/home/ftpusers/anonymous#  extundelete  ~/image/xubuntu.img
--restore-all
```

Obnovené hľadané súbory sú uložené v adresári *RECOVERED_FILES/home/ftpusers/anonymous*. Všetkých päť súborov sa podarilo obnoviť.

```
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# ls
DSC03178.jpg  DSC03205.jpg  DSC03248.jpg  DSC03503.jpg  file.zip
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous#
```

Štyri súbory zachytávajú obrázky prírody, piatym je archív typu zip.

3. Detekcia steganografie v súboroch typu jpg

Steganografia je metóda skrývania dát. Pri steganografii je cieľom nielen utajiť obsah správy, ale aj správu samotnú. Ide teda o skrytie prenášanej informácie tak, aby o jej existencii nevedel okrem odosielateľa a prijímateľa nikto iný. V princípe je tajná správa (message) vložená do oveľa väčšieho súboru (carrier) a spracovaná spôsobom špecifickým steganografickému algoritmu tak, aby pozmenený cieľový súbor bol interpretovaný na nerozoznanie od originálneho. Ako nosič sa zvyčajne využívajú mediálne súbory. Sú preferované kvôli svojej bežnosti a rozšírenosti, takže nevzbudzujú dojem že nesú tajnú informáciu. Rovnako sú to typicky veľké súbory, takže sú schopné poňať väčšie množstvo tajnej informácie.

a. Zmeňte pracovný adresár na adresár v ktorom sú obnovené súbory z predchádzajúceho kroku.
b. Využitím nástroja stegdetect overte prítomnosť skrytej správy v súboroch typu jpg a program, ktorým bola správa zabudovaná.
c. Použitím vyhľadávacieho nástroja vyhľadajte tento open source program na internete a pokúste sa o obnovenie skrytej informácie. Neuvažujte ochranu heslom.
d. Podľa štruktúry súboru určite jeho typ a zobrazte ho v odpovedajúcom nástroji. Hlavičky známych súborov je možné zistiť z konfiguračného súboru programu scalpel (*/etc/scalpel/scalpel.conf*).

Zmena pracovného adresára sa vykoná príkazom _____.
Program stegdetect detekoval použitie metódy vstavania informácie vlastnej programu _____.
Skrytú informáciu sa podarilo obnoviť spustením _____.
Hlavička extrahovaných súborov v hexa editore je_____.
Vstavanou informáciou sú _____.

Riešenie:

Počas obnovy všetkých súborov boli tieto uložené do adresára *RECOVERED_FILES*, pričom cesta každého súboru ostala zachovaná. Zmenu pracovného adresára vykonáme podobne ako v minulých krokoch.

```
root@bt:~# cd RECOVERED_FILES/home/ftpusers/anonymous/
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous#
```

V adresári sa nachádzajú štyri súbory typu jpg. Program stegdetect spustený bez parametrov sa pokúsi o detekciu vstavanej informácie a identifikuje nástroj, ktorým bola táto informácia vstavaná.

```
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# ls -a
.  ..  DSC03178.jpg  DSC03205.jpg  DSC03248.jpg  DSC03503.jpg  file.zip
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# stegdetect *.jpg
DSC03178.jpg : f5(***)
DSC03205.jpg : f5(***)
DSC03248.jpg : f5(***)
DSC03503.jpg : f5(***)
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous#
```

Program F5 je voľne dostupný nástroj ktorý dokáže informáciu do jpg súboru vložiť a aj extrahovať. V čase písania dokumentu je dostupný spolu s príkladom použitia na stránkach projektu http://code.google.com/p/f5-steganography/.

Extrakcia vstavanej informácie je vykonaná spustením programu s parametrom *x* pre každý súbor zvlášť.

```
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# java -jar f5.jar x -e 01
DSC03178.jpg
Huffman decoding starts
Permutation starts
10616832 indices shuffled
Extraction starts
Length of embedded file: 34498 bytes
(1, 15, 4) code used
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous#
```

Výstup je uložený v súbore *01*. Zobrazením súboru v hexa editore podľa hlavičky vidíme že ide znova o súbor jpg, ktorý je možné zobraziť integrovaným prehliadačom obrázkov v distribúcii BackTrack.

```
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous# hexedit 01
00000000   FF D8 FF E0  00 10 4A 46  49 46 00 01  01 01 00 60  00 60 00 00
FF E1 00 C0  ......JFIF.....`.`......
00000018   45 78 69 66  00 00 49 49  2A 00 08 00  00 00 05 00  1A 01 05 00
01 00 00 00  Exif..II*.............
00000030   4A 00 00 00  1B 01 05 00  01 00 00 00  52 00 00 00  28 01 03 00
01 00 00 00  J...........R...(.......
```

Hlavičku jpg súborov zistíme z konfiguračného súboru nástroja na obnovu dát *scalpel*.

```
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous#                      cat
/etc/scalpel/scalpel.conf  | grep jpg
#     jpg     y       5000:100000     \xff\xd8\xff\xe0\x00\x10        \xff\xd9
      jpg     y       200000000       \xff\xd8\xff\xe0\x00\x10        \xff\xd9
      jpg     y       200000000       \xff\xd8\xff\xe1                \xff\xd9
root@bt:~/RECOVERED_FILES/home/ftpusers/anonymous#
```

Ukončenie práce

Po ukončení práce odstráňte všetky vytvorené súbory a počítač vypnite príkazom

```
root@bt:~# shutdown -h now
```